Transaktionskosten der Nutzung des Internet durch Missbrauch (Spamming) und Regulierungs-möglichkeiten

Franz Büllingen
Annette Hillebrand
Peter Stamm

Nr. 272

Januar 2006

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68, 53604 Bad Honnef
Postfach 20 00, 53588 Bad Honnef
Tel 02224-9225-0
Fax 02224-9225-63
Internet: http://www.wik.org
eMail info@wik.org
Impressum

In den vom WIK herausgegebenen Diskussionsbeiträgen erscheinen in loser Folge Aufsätze und Vorträge von Mitarbeitern des Instituts sowie ausgewählte Zwischen- und Abschlussberichte von durchgeführten Forschungsprojekten. Mit der Herausgabe dieser Reihe bezweckt das WIK, über seine Tätigkeit zu informieren, Diskussionsanstöße zu geben, aber auch Anregungen von außen zu empfangen. Kritik und Kommentare sind deshalb jederzeit willkommen. Die in den verschiedenen Beiträgen zum Ausdruck kommenden Ansichten geben ausschließlich die Meinung der jeweiligen Autoren wieder.

ISSN 1865-8997

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BEP	Break-Even-Point
BGH	Bundesgerichtshof
BNetzA	Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDV	Deutscher Direktmarketing Verband e.V.
DMP	Designated Mailers Protocol
Eco	Electronic Commerce Forum - Verband der deutschen Internetwirtschaft e.V.
ENUM	Telephone Number Mapping
EU	Europäische Union
ICANN	Internet Corporation For Assigned Names and Numbers
ICCP	OECD Committee for Information, Computer and Communications Policy
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
MDStV	Mediendienste-Staatsvertrag
MMS	Multimedia Messaging Service
MTA	Mail Transfer Agent
MWD	Mehrwertdienste
MWDG	Mehrwertdienstegesetz
OECD	Organisation for Economic Co-operation and Development
ORDB	Open Relay Database
PSTN	Public Switched Telephone Network
RBL	Real Time Blacklist
RegTP	Regulierungsbehörde für Telekommunikation und Post
RMX	Reverse Mail eXchange
SIP	Session Initiation Protocol
SMPT	Simple Mail Transfer Protocol
SMS	Short Message Service
SPF	Sender Policy Framework
Spit	Spam over Internet Telephony
StGB	Strafgesetzbuch

TDDSG	Gesetz über den Datenschutz bei Telediensten
TDG	Gesetz über die Nutzung von Telediensten
UN	United Nations
UWG	Gesetz gegen den unlauteren Wettbewerb
VoIP	Voice over IP
VOIPSA	Voice-over-IP-Security Alliance
WSIS	World Summit on the Information Society
ZAW	Zentralverband der deutschen Werbewirtschaft ZAW e.V.

Zusammenfassung

Unerwünschte Massenaussendungen besitzen kommerziellen Charakter und werden über Telefon ebenso versendet wie über Fax, Post und insbesondere E-Mail. Seriöses Direktmarketing über E-Mail stellt demgegenüber einen wichtigen Zweig der Werbewirtschaft dar. Im Jahr 2003 wurden 1,9 Mrd. Euro für diese Form der Werbung ausgegeben. Auch in Zukunft ist mit einem hohen Interesse der Werbewirtschaft zu rechnen, diese kostengünstige Werbeform zu nutzen. Spam macht heute bis zu 80 Prozent aller versandten E-Mails aus. Dies bedeutet ein Spam-Aufkommen von schätzungsweise 48 Mrd. weltweit pro Tag in 2005. Der Großteil des Spam stammt aus den USA sowie Südkorea. Nur etwa 2 Prozent werden von Deutschland aus verschickt. Diese Tatsache erschwert die strafrechtliche Verfolgung der Spammer erheblich.

Eine für die Nutzer häufig mit hohen Schäden verbundene Art von Spam ist das Rufnummern-Spamming. Auf Grundlage des TKG und des MWD-Gesetzes ist die BNetzA befugt, gegen den Missbrauch vorzugehen. Die verschiedenen Sanktionen reichen allerdings nicht aus, um eine abschreckende Wirkung für Spammer zu entfalten. Auf nationaler Ebene wurden Gesetze und regulatorische Maßnahmen ergriffen, die die entsprechenden EU-Richtlinien umsetzen. Dazu gehört in Deutschland die Novellierung des UWG. Um Rufnummern-Spamming gezielt zu bekämpfen, wurde das Mehrwertdienste-Gesetz (MWD-Gesetz) verabschiedet. Ergänzt werden diese Maßnahmen durch selbstregulative Initiativen der Verbände wie etwa die Beschwerde-Hotlines von Eco, VZBV, WBZ, die Einführung von Whitelists (Certified Senders Alliance mit Code of Conduct) sowie durch das „Aktionsbündnis gegen Spam“.

Aufgrund der geringen Kosten für den Versand von E-Mails existieren hohe Anreize, das Medium zu missbrauchen, so dass kaum mit einem dauerhaften Rückgang von Spam zu rechnen ist. Bei E-Mail-Spam reichten rechnerisch bereits 0,02 Kunden pro 1.000 angemailter Adressen und einer Auftragsspanne von 50 Euro, um den Break-Even zu erreichen. Die volkswirtschaftlichen Kosten für Spam und andere Formen von unerwünschten Massenaussendungen haben daher erheblich zugenommen, so dass Handlungsbedarf auf nationaler und internationaler Ebene besteht.

Zahlreiche Akteure und neugegründete Initiativen haben sich inzwischen des Spamproblems angenommen. Durch Aktivitäten auf der politischen, rechtlichen und sozialen Ebene versuchen sie, die Funktionabilität von E-Mail wieder zu erhöhen, die durch Spam verursachten Kosten für ISP und Nutzer zu verringern und gleichzeitig das Internet als Form des Direktmarketings zu erhalten. Eine Verminderung von Spam ist daher nur durch ein Zusammenspiel von Gegenmaßnahmen auf verschiedenen Ebenen möglich. Dazu gehören internationale Kooperationen genauso wie Gesetze und regulatorische Maßnahmen auf nationaler Ebene, Selbstregulierung, technische Maßnahmen sowie eine intensive Informierung der Nutzer.

Summary

Unrequested mass mailings are characterized by being sent via phone, as well as by fax, mail and particularly via e-mail. In contrast serious electronic direct marketing represents an important branch of the advertising industry. In 2003 1.9 billion euros were spent on this kind of promotion. It has to be taken into account that in future this type of advertising will still be of growing interest for the advertising industry. Today spamming constitutes up to 80 per cent of all outgoing e-mails. This means a spam quantity of approximately 48 billion occurs worldwide per day in 2005. The largest deal of spam is originated from the USA and South-Korea. Only around two per cent of spam is being sent from Germany. This fact opposes seriously against criminal prosecution of spamming by national authorities.

One kind of misuse associated with serious disadvantages for users is spamming by phone. Based on the Telecommunications Law (TKG) and the Law for Value Added Services (Mehrwertdienste-Gesetz), the German regulatory authority BNetzA is authorised to act against misuse. However different means of sanctions are not sufficient for displaying deterrent effects on spamming. On national level, laws and regulatory measures were taken, which implement the corresponding EU guidelines. This includes the amendment of the Law Against Unfair Competition (UWG) in Germany. In order to fight spamming by phone effectively, the Law for Value Added Services was passed. These measures are supplemented by self-regulative initiatives of associations such as “Complain Hotlines” of different associations like Eco, VZBV and WBZ, the introduction of white lists (Certified Senders Alliance on behalf of a Code of Conduct) as well as by the so called „Aktionsbündnis gegen Spam“.

Due to the marginal costs of dispatching mass e-mails, high incentives stimulate the misuse of the medium. So the decline of mass spam hardly will be seen. With e-mail spam 0.02 customers per 1.000 placing an order with a value of 50 euros on average will be already sufficient in order to achieve the break-even. Therefore transaction costs of spam and any other forms of unrequested mass mailings have increased substantially. Most experts are convinced that there is strong need for action on national and international level.

Meanwhile a large number of actors and political initiatives have given mind to spamming problems. Taking action on political, legal, and social levels these initiatives try to preserve the availability and functionality of the e-mailing system in order to reduce costs for ISPs and users. At the same time some of these actors try to keep up the internet as an important medium of direct marketing. This means that the reduction of spamming is difficult and only feasible by interacting counteractive measures on different levels.

This includes international co-operation and co-ordination as well as regulatory activities on the national level, self-regulation of branch actors, technical measures and an intensified dialog with Internet users.

1 Einleitung

E-Mails zählen zu den Killerapplikationen des Internet und haben während der letzten zehn Jahre dessen Diffusion wesentlich vorangetrieben. Der E-Mail-Dienst stellt heute ein zentrales Kommunikationsmedium bei den privaten und professionellen Anwendern dar. Der Erfolg von E-Mail beruht neben Schnelligkeit und Asynchronität vor allem auf den Transaktionskostenvorteilen gegenüber Briefpost, Telefax und Telefonie. Zudem erfolgen dank E-Mail nicht nur eine Substitution traditioneller Kommunikationsmedien, sondern auch eine deutliche Zunahme der Kommunikation und eine Vereinfachung von Organisations- und Koordinationsprozessen.

Die Erfolgsgeschichte des E-Mail-Dienstes wird jedoch in jüngerer Zeit immer stärker durch Missbrauchsphänomene bedroht. Es werden massenhaft unerwünschte E-Mails, sog. Spam-Mails verschickt, gegen die sich die Empfänger kaum zur Wehr setzen können und die im harmlosen Fall Werbeinhalte, im schlimmsten Fall gefährliche Computerviren und Betrügereien verbreiten. Zum Teil erfolgt der Versand dieser Spam-Mails mit missbräuchlich bemächtigten Absenderadressen, die beim Empfänger den Eindruck erwecken sollen, Nachrichten bekannter oder vertrauter Kommunikationspartner erhalten zu haben.

Um den Zeitaufwand für das Aussortieren der unerwünschten E-Mails sowie Spam-Traffic zu reduzieren verwenden die Internet Service Provider (ISP), welche E-Mail-Dienste anbieten, und zum Teil auch die Nutzer selbst, Softwaretools zur automatischen Blockade von Spam. Die hierbei dezentral gepflegten Blacklists mit unerwünschten Absenderadressen bergen das Risiko falscher Zuordnungen, wodurch die Zuverlässigkeit der E-Mail-Übermittlung stark eingeschränkt wird.

Experten sprechen bereits davon, dass gegenwärtig etwa 80 Prozent aller versendeten E-Mails Spam-Mails darstellen, wodurch die Qualität und Zuverlässigkeit des Mediums nachhaltig gemindert wird. Der volkswirtschaftliche Schaden wurde bereits in einem EU-Kommissionsbericht 2003 weltweit auf rd. 10 Mrd. Euro geschätzt. Bis 2009 wird sogar eine Verzehnfachung dieser Kosten für Abwehrmaßnahmen und verlorene Produktivität prognostiziert.

Ziel dieser Studie ist die Darstellung von Lösungsansätzen zur Verhinderung der Missbräuche sowie die Prüfung und Bewertung von geeigneten Regulierungsmöglichkeiten.

Im Einzelnen wird dargelegt, welche nationalen und internationalen Gremien und Verbände sich mit dieser Problematik befassen. In diesem Zusammenhang werden die Interessenslagen der Internetwirtschaft und E-Mail-Nutzer auf Gemeinsamkeiten und Konflikte hin überprüft.

Darauf aufbauend werden technische, ökonomische und regulatorische Lösungsansätze zur Eindämmung von Spam-Mails und zur Erhöhung der Zuverlässigkeit des E-Mail-Dienstes vorgestellt und bewertet werden.

Zuvor wird jedoch eine Definition der verschiedenen Begrifflichkeiten im Zusammenhang mit unerwünschten Massenaussendungen vorgenommen und die dahinter liegenden Geschäftsmodelle dargestellt. Außerdem wird das von Spam ausgehende Bedrohungspotenzial ausführlich analysiert.

Die Analyse der Abwehrstrategien gegen E-Mail-Missbrauch erfolgte auf der Basis von Auswertungen aktueller Meldungen, Literaturstudien, Informationen aus dem Internet, Gremienberichten sowie Experteninterviews. Für die Abschätzung der wirtschaftlichen Schäden wurden transaktionskostentheoretische Ansätze hinzugezogen.

2 Missbrauchsmöglichkeiten moderner Kommunikationsmittel durch unerwünschte Massenaussendungen: Spam, Spit und andere

2.1 Ausgangslage

Immer häufiger erhalten Internet-Nutzer unerwünschte Werbung, die mittels E-Mails massenhaft verbreitet wird. Betroffen sind sowohl private als auch gewerbliche Nutzer. In der Internet-Community hat sich schon frühzeitig der Begriff „Spam“ für diese Art von elektronischem Werbemüll etabliert. Als vor etwa 10 Jahren zwei US-Rechtsanwälte aus Phoenix, Arizona, an rund 6.000 Newsgroups Werbemails sandten, ist der Begriff erstmals einer breiteren Öffentlichkeit bekannt geworden.[1] Der Umfang dieses Spamming mutet heute als geradezu verschwindend gering an. Derzeit löschen viele Nutzer täglich einige Dutzend oder gar Hunderte solcher Spam-Mails aus ihrem Account.

Von Spam spricht man im Allgemeinen, wenn E-Mails kommerziellen Charakter haben und der Empfang unerwünscht ist. Der Missbrauch moderner Kommunikationsmedien ist jedoch nicht auf E-Mail beschränkt. Auch über (Mobil-)Telefon oder Fax werden unerwünschte Botschaften verbreitet. Rechtliche, organisatorische und technische Gegenmaßnahmen richten sich daher nicht nur gegen Spam, sondern in der Regel gegen alle Formen unerwünschter Massenaussendungen. In der Diskussion wird aber der Begriff „Spam“ unrichtigerweise häufig als Synonym für E-Mail-Werbung, Werbung über elektronische Medien oder auch für jede Art von unerwünschten Nachrichten verwandt.

Es erscheint daher notwendig, in der vorliegenden Studie die verschiedenen Begriffe im Zusammenhang mit dem Missbrauch elektronischer Medien einerseits sowie der rechtmäßigen Verwendung dieser Medien für Direktwerbung andererseits zu definieren und gegeneinander abzugrenzen.

Eine Definition soll vor dem Hintergrund folgender Aspekte vorgenommen werden:

- dem Interesse des Verbrauchers, nur dann Werbung zu erhalten, wenn er zuvor in die Verwendung seiner Adresse für diese Zwecke eingewilligt hat (Datenschutz),
- den Interessen der Werbetreibenden an seriösen Formen des Direktmarketings,
- dem Interesse aller Privat- und Geschäftskunden von elektronischen Diensten an der Erhaltung der Funktionabilität und Verlässlichkeit der Kommunikationssysteme,
- der Vermeidung von negativen externen Effekten und damit Kosten für die Nutzer durch unerwünschte Kommunikation.

---

1 Vgl. Barret (1996).

2.2 Definition unerwünschte Massenaussendungen

Mit der Invention moderner elektronischer Kommunikationsmedien und der zunehmenden Verbreitung von Empfangsgeräten für diese Dienste insbesondere bei privaten Nutzern geht das Phänomen einher, dass diese Kommunikationskanäle missbraucht werden. Jedes Netz wird mit Erreichen einer kritischen Masse auch attraktiv für unseriöse Sender von Werbebotschaften und betrügerischen Mitteilungen, die ohne das Einverständnis des Empfängers agieren.

Die verschiedenartigen Phänomene sollen unter dem Begriff **unerwünschte Massenaussendungen** zusammengefasst werden. Damit ist zunächst offen, ob es sich um Inhalte handelt, die prinzipiell legal sind (z. B. Werbung) oder um illegale Inhalte (z. B. gefälschte SMS-„Kontaktanzeigen").

Unerwünscht sind Sendungen dann, wenn der Nutzer nicht in die Verwendung seiner Kommunikationsadressen für diese Mitteilungen eingewilligt hat (opt-in) bzw. eine allgemeine Gesetzesgrundlage das Senden von Kommunikationsinhalten unter bestimmten Prämissen gestattet.[2]

Es ist demnach zu unterscheiden zwischen unerwünschten Massenaussendungen, bei denen das Aussenden prinzipiell legaler Inhalte eine illegale Handlung darstellt, z. B. weil dieses Senden einen Verstoß gegen die Datenschutzbestimmungen darstellt, und Massenaussendungen, bei denen sowohl das Aussenden an sich als auch die Inhalte Ordnungswidrigkeiten oder Straftaten darstellen können (*unerwünschte Massenaussendungen mit legalem Inhalt / unerwünschte Massenaussendungen mit illegalem Inhalt*).

In die erste Kategorie der **unerwünschten Massenaussendungen mit legalem Inhalt** fallen zum Beispiel E-Mails durch Produktanbieter, denen gegenüber der Adressat nicht in die Verwendung seiner E-Mail-Adresse für Werbezwecke eingewilligt hat, der Inhalt der Kommunikation jedoch rechtlich nicht zu beanstanden ist. In die zweite Kategorie der **unerwünschten Massenaussendungen mit illegalem Inhalt***,* gehören beispielsweise E-Mails, die in betrügerischer Absicht Werbung für (0)190er/(0)900er Nummern (missbräuchliche Anwählprogramme[3]) verbreiten.

---

2 Eine Prämisse ist beispielsweise erfüllt, wenn das Unternehmen eine dauerhafte Kundenbeziehung zu dem Adressaten unterhält. In den EU-Mitgliedsländern ergeben sich die rechtlichen Rahmenbedingungen für das Versenden von Werbung aus der Datenschutzrichtlinie 2002/58/EG.

3 Der übliche Begriff für Anwählprogramme „Dialer" wird fälschlich in der Presse zunehmend so verwandt, als handele es sich dabei prinzipiell um illegale Einwählprogramme. Dass diese Programme für viele legale und erwünschte Mehrwertdienste genutzt werden, wird dabei oft übersehen. Im Folgenden soll der Begriff (MWD-)Rufnummernmissbrauch verwendet werden (bzw. missbräuchliche Anwählprogramme, Dialer-Missbrauch).

2.3 Definition erwünschte Massenaussendungen (Direktmarketing)

Grundsätzlich können Massenaussendungen aus

- Sprache oder
- Text

bestehen. Dabei ist zu beachten, dass der weitaus größte Teil von seriösen Werbetreibenden stammt, die verschiedene Medien erfolgreich für die direkte, kostengünstige und erwünschte Ansprache ihrer (potenziellen) Kunden nutzen. Jährlich wenden Unternehmen in Deutschland nach Angaben des Branchenverbands DDV zweistellige Milliardenbeträge für Direktmarketing auf. Im Jahr 2003 summierten sich die Ausgaben auf 30,8 Mrd. Euro, was ein Zuwachs von 6,2 Prozent gegenüber dem Vorjahr bedeutet.[4]

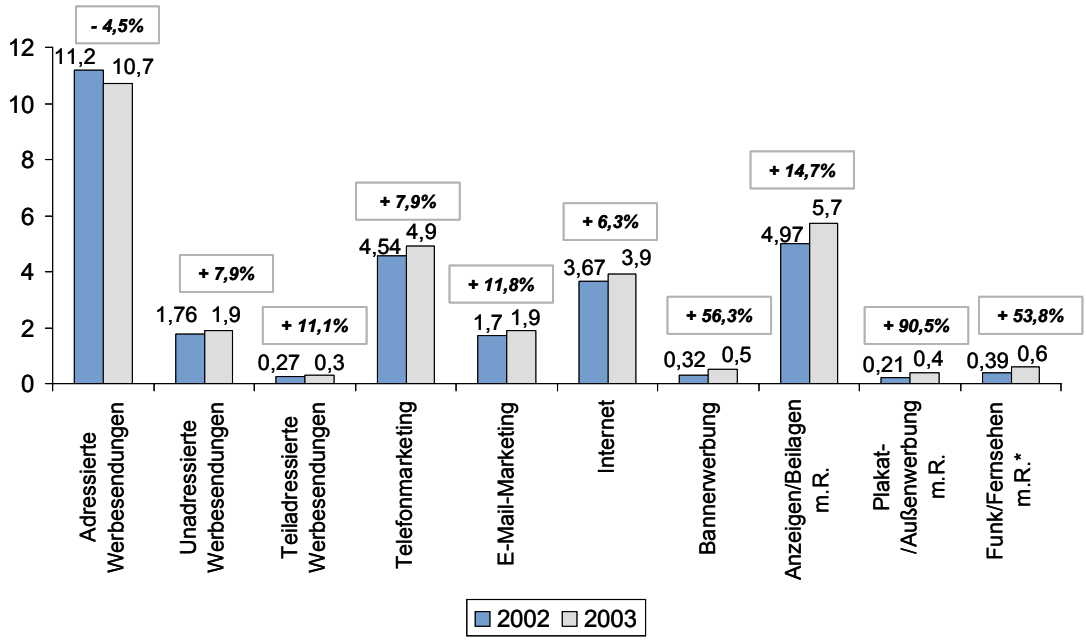
Welcher Übertragungsweg für die Werbung gewählt wird, hängt vor allem davon ab, welche Zielgruppe erreicht werden soll und welche Kosten die Verbreitung verursacht. Im Direktmarketing[5] werden potenzielle Kunden immer noch häufig über herkömmliche Briefe und (größtenteils analoge) Faxgeräte kontaktiert. So nehmen die Aufwendungen für adressierte (Post-)Werbesendungen im Jahr 2003 mit 10,7 Mrd. Euro einen Spitzenplatz ein, gefolgt von Werbungen über Anzeigen/Beilagen mit Antwortelementen (vgl. Abbildung 2-1). Der traditionelle Bereich der adressierten Werbung über den Briefkasten ist jedoch rückläufig (im Vergleich zu 2002 -4,5 Prozent).

---

4 Die erhebliche Bedeutung von Online-Medien im Direktwerbemarkt wird auch daran deutlich, dass die Nettowerbeeinnahmen erfassbarer Werbeträger im Online-Bereich im Jahr 2004 mit 271 Mio. Euro vergleichsweise gering waren (zum Vergleich: Tageszeitungen 4,5 Mrd. Euro, TV 3,86 Mrd. Euro), vgl. ZAW 2005.

5 Zum Direktmarketing zählen adressierte, unadressierte (z. B. Postwurfsendungen) und teiladressierte (z. B. an Bewohner einer best. Straße) Werbesendungen (papierbasiert), das Telefonmarketing (dazu zählen aktive Anrufe z. B. eines Call Centers und passive Anrufe, d.h. Anrufe des Verbrauchers beim Unternehmen, aber auch Fax), E-Mail-Marketing (z. B. über Newsletter (regelmäßig) oder E-Mailings (aktionsbezogen)), Internet (z. B. über Dialer), Bannerwerbung (z. B. verbunden mit Links) sowie Anzeigen/Beilagen, Plakat/Außenwerbung und Funk/Fernsehen, jeweils mit Responseelementen (vgl. Systematik des DDV unter http://www.direktmarketing-info.de).

Abbildung 2-1: Aufwendungen nach Direktwerbemedien 2002 und 2003 in Deutschland (in Mrd. Euro)



Quelle: DDV (Deutscher Direktmarketing Verband) 2005 (* mit Responseelement)

Die Preissenkungen in der Sprachtelefonie haben dazu geführt, dass vermehrt auch Telefonate – zumeist über Festnetzanschlüsse – für Werbebotschaften und vor allem auch Call Center Services genutzt werden. Mobilfunkanschlüsse werden dagegen weniger mit Sprach- sondern eher mit Textnachrichten (SMS) beworben. Insgesamt ist in Bezug auf Telefonmarketing eine steigende Tendenz beobachtbar. Die Anzahl der per Anruf vermittelten Werbebotschaften nahm im Jahr 2003 im Vergleich zum Vorjahr um 7,9% zu (2002: 4,54 Mrd. Euro, 2003: 4,9 Mrd. Euro). Insgesamt fällt auf, dass Werbung im Bereich der Online-Medien und Werbung mit Responseelementen[6] die höchsten Zuwachsraten zu verzeichnen hat. Dies deutet auf eine zunehmende Relevanz von Interaktion über elektronische Medien hin. Aufmerksamkeit wird über traditionelle Werbeformen generiert, aber diese werden zunehmend mit Interaktionsangeboten angereichert, um Kunden individueller anzusprechen.

Die geringen Kosten für E-Mail können als eine zentrale Ursache dafür gesehen werden, dass E-Mail in den letzten zwei Jahren zu einem wichtigen neuen Medium der Direktwerbung avanciert ist. Diese E-Mailings sind das elektronische Pendant zu traditionellen Direct Mailings per Briefpost. Im Gegensatz zu Newslettern werden E-Mailings

6 Bei den Responseelementen dominieren die elektronischen Medien wie Telefon, SMS und E-Mail.

nicht periodisch, sondern aktionsbezogen versendet. Der Begriff E-Mailings wird daher im Weiteren als seriöses Pendant zum Begriff „Spam“ verwandt. Die Ausgaben dafür stiegen von 2002 auf 2003 um 11,8 Prozent auf 1,9 Mrd. Euro.

2.4 Definition Missbrauchsformen von Direktmarketing

Alle Medien der Direktwerbung können von unseriösen Anbietern auch missbräuchlich verwendet werden. Je mehr Teilnehmer ein Medium hat und je kostengünstiger es genutzt werden kann, desto höher ist scheinbar auch das Missbrauchspotenzial, wie die jüngste Entwicklung im Bereich E-Mail und Telefonie/SMS zeigt.

2.4.1 Missbrauch bei Telefonmarketing und E-Mail-Marketing

Im Fokus dieser Studie sollen daher die Missbrauchsmöglichkeiten der folgenden elektronischen, direkt adressierten Werbeformen stehen: Telefonmarketing und E-Mail-Marketing.[7]

1. Missbrauchsformen bei Telefonmarketing

- **automatische Anrufmaschinen**: Anrufautomaten generieren mit marginalen Kosten zufällige Telefonnummern, um Werbebotschaften zu verbreiten. Dabei werden nicht nur Nummern gewählt, die in Verzeichnissen gelistet sind, sondern auch Zufallskombinationen. Angeblich sind bis zu 1.000 Anrufe pro Minute möglich. Verfahren dieser Art spielen in Deutschland zurzeit keine Rolle, in anderen Ländern wie z. B. Großbritannien und den USA sind sie erlaubt und werden häufig eingesetzt. Künftig könnte sich diese Form des Direktmarketings weltweit noch stärker verbreiten, da dramatische Kostensenkungen in der Sprachtelefonie durch die Diffusion der Internet-Telefonie (Voice over IP – VoIP) zu erwarten sind. Technisch ist die Verbreitung von unerwünschten Werbebotschaften über VoIP beinahe vollständig automatisierbar (vgl. Spit).
- **Ping-/Lock-Anrufe**: Ein Anschluss wird kurz angewählt mit dem Ziel, eine Nummer in der Rückruflisten-Funktion des Nutzers zu platzieren. Der Rückruf dient z. B. dem Ziel, Werbebotschaften zu adressieren. Eine weiter gehende Missbrauchsmöglichkeit besteht darin, den Rückruf über Mehrwertdienste (MWD)-Rufnummern zu leiten.
- **unerwünschte SMS**: Neben der einfachen Versendung von unerwünschten Werbe-SMS setzt sich eine Missbrauchsmöglichkeit immer mehr durch, bei der eine SMS dem Ziel dient, weitere SMS-Antworten zu generieren (auch kombiniert mit MWD) (Beispiel: falsche „Kontaktbörsen“).

---

7 Das Bedrohungspotenzial dieser Werbeformen wird in Abschnitt 6 analysiert.

- **unerwünschte Faxmitteilungen**: Bei der Versendung von Werbebotschaften über Faxgeräte sind grundsätzlich alle Missbrauchsformen wie bei Telefonie oder SMS denkbar. Die Menge der unerwünschten Massenaussendungen per Fax scheint aufgrund der sinkenden Bedeutung des Mediums für die Geschäftskommunikation zurückzugehen.
- **Spit**: „SPam over Internet Telephony" gilt als ernstzunehmende künftige Bedrohung, vor allem da durch die weitere Verbreitung von VoIP Werbeanrufe unabhängig vom Standort des Senders noch günstiger werden. Wie bei E-Mail-Spam gibt es auch hier Techniken, um Nachrichten automatisch in großer Zahl zu verschicken. Zudem erlaubt VoIP die Generierung der Anrufe zu Grenzkosten aus dem Ausland, so dass die Rückverfolgung der Verursacher wie auch bei Spam nahezu aussichtslos erscheint.

2. Missbrauchsformen bei E-Mail-Marketing

- **Spam**: Der Begriff „Spiced Pork And Meat" für in Gelee eingelegtes Frühstücksfleisch wird seit vielen Jahren für massenhaft versandte, unerwünschte E-Mails[8] verwendet. Daneben existieren noch die rechtlich-technischen Bezeichnungen UBE (Unsolicited Bulk E-Mail) und UCE (Unsolicited Commercial Electronic Mail). UBE ist massenhaft versandte unerwünschte E-Mail, der Begriff UCE betont den kommerziellen Charakter der Zusendungen.

2.4.2 Rufnummernmissbrauch

Sowohl unseriöse Formen des Telefonmarketings als auch des E-Mail-Marketings haben in jüngster Zeit an Brisanz gewonnen, da die unerwünschten Nachrichten und Werbesendungen immer häufiger mit Formen des Rufnummernmissbrauchs kombiniert werden. **Rufnummernmissbrauch** liegt dann vor, wenn Rufnummern nicht in der gesetzlich bzw. behördlich vorgeschriebenen Weise genutzt werden. In Deutschland ist in diesem Fall die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) (vormals Regulierungsbehörde für Telekommunikation und Post – RegTP) sanktionsbefugt. Aufgrund der zunehmenden Konvergenz der Medien macht die Agentur keinen Unterschied, wie die unverlangt eingesandte Nachricht den Verbraucher erreicht. Rufnummernmissbrauch in Kombination mit unerwünschten Massenaussendungen über Fax, (Telefon-)Rückruf, SMS oder E-Mail fasst die Agentur unter dem Begriff „**Rufnummern-Spamming**" zusammen. Falls eine Rufnummer in einer

---

8 E-Mail ist nur eine Form elektronischer Post. Der Begriff elektronische Post schließt auch SMS, MMS und jegliche Form elektronischer Kommunikation ein, die keine gleichzeitige Teilnahme von Sender und Empfänger erfordert (vgl. Kommission der Europäischen Gemeinschaften (2004)). Spam wird in dieser Studie nicht als Oberbegriff für unverlangt zugesandte Nachrichten, sondern nur im Zusammenhang mit unerwünschter E-Mail verwendet.

elektronischen Nachricht angegeben ist, fällt eine evtl. Beschwerde über diese Nachricht in die Zuständigkeit der BNetzA.[9]

Immer öfter weisen Sendungen im Zusammenhang mit Telefon- oder E-Mail-Marketing auf Mehrwertdienste-Rufnummern hin oder es werden unbemerkt vom Nutzer Verbindungen zu diesen kostenpflichtigen Rufnummern hergestellt. Häufig animieren Werbebotschaften per E-Mail dazu, über eine MWD-Nummer ((0)190er/(0)900er Nummer oder auch Auslands- und Satellitenrufnummern) Rückrufe zu starten. Diese Versendung von unerwünschten Nachrichten verfolgt das Ziel, über die Rückrufe dem unseriösen Anbieter zu Einnahmen aus MWD-Entgelten zu verhelfen. Besonders problematisch sind E-Mails, bei denen über Anhänge oder über Links das unbemerkte Einwählen über einen Dialer provoziert wird. Allerdings überprüft die Bundesnetzagentur nicht die unter Mehrwertdiensterufnummern angebotenen Dienste auf ihren Inhalt. Die Qualität der Dienstleistung wird von der Bundesnetzagentur ebenso wenig wie das Preis-Leistungs-Verhältnis bewertet.

Zu Rückrufen kann prinzipiell über jedes Medium animiert werden. Die zahlreichen Beschwerden über stark überhöhte TK-Entgeltabrechnungen belegen, dass das Problem des Rufnummernmissbrauchs immer häufiger auftritt (vgl. Abbildung 2-2)[10] und einen wesentlichen Teil der unerwünschten Massenaussendungen sowohl im Hinblick auf die Quantität als auch die Qualität in Form finanzieller Schäden ausmacht. Allerdings geschieht der Missbrauch von MWD-Rufnummern zurzeit noch hauptsächlich via Fax (47% der Beschwerden) und per Rückruf[11] (40% der Beschwerden) und weniger per SMS (12%) oder E-Mail (2%) wie die Beschwerdestatistik der BNetzA zeigt.[12]

Seit Inkrafttreten des MWDG am 15. August 2003 erreichten den Verbraucherservice 2.496 Anfragen und Beschwerden zu dieser Thematik bis zum Ende des Jahres 2003 (d.h. im Mittel 555 pro Monat). Neben allgemeinen Anfragen zum Gesetz wurden Nachfragen zur Registrierung eines Dialers und zur Herangehensweise bei der Ermittlung des Rufnummerninhabers beantwortet. Im Jahr 2004 sind insgesamt 3.703 Beschwerden eingegangen (d.h. im Mittel 308 pro Monat).

Diese Zahl wird sich für das Jahr 2005 deutlich erhöhen. Die Zahl der bei der BNetzA im ersten Halbjahr 2005 eingegangenen Beschwerden über Spam beträgt 9.790. Im zweiten Halbjahr 2005 nahm die Beschwerdeflut weiter zu. Die BNetzA schätzt die An-

---

9 Vgl. RegTP Jahresbericht 2004, S. 7.

10 Im Jahr 2004 gingen bei der BNetzA 4.927 Beschwerden dazu ein (vgl. ebenda). Ein Vergleich zum Vorjahr ist schwierig, da entsprechende Statistiken nicht zur Verfügung stehen. Die BNetzA ist seit dem 15.08.2003 mit der Umsetzung des MWDG betraut. Seit diesem Zeitpunkt gingen rd. 850 Beschwerden zu (0)190er/(0)900er Mehrwertdiensterufnummern bei der Agentur ein.

11 Dabei klingelt das Telefon des Angerufenen nur kurz. Bei Betätigung der Rückruftaste wird dann ein Anruf zu einer MWD-Rufnummer erzeugt.

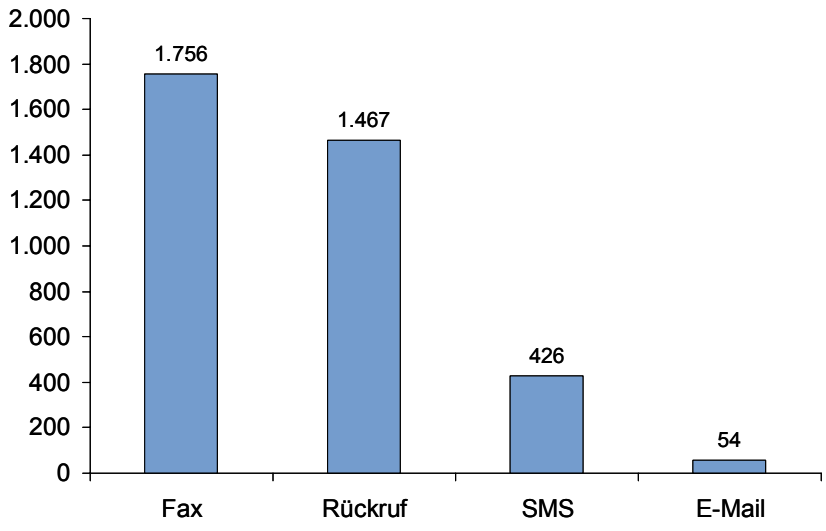
12 Die Statistik gibt jedoch nur ein unvollständiges Bild, da nur die Fälle erfasst werden, bei denen Beschwerden bei der Agentur eingegangen sind.

zahl der Beschwerden für das Gesamtjahr auf bis zu 25.000.[13] 7 Prozent davon entfallen auf E-Mail, 40 Prozent auf Fax und die übrigen 53 Prozent auf SMS, Ping-Anrufe, automatisierte Anrufe mit Gewinnversprechen u.ä.

Da sich Sachverhalte zum Teil überschneiden – manchmal werden zu einem Fax einige Hundert Beschwerden an die BNetzA gesandt – ist nicht jede Beschwerde mit einem Fall für die Behörde verbunden. Einen erheblichen Aufwand stellt die Beantwortung der Beschwerden aber dennoch dar, nicht zuletzt weil auch jeder Anfragende eine Eingangsbestätigung seines Schreibens erhält.

Die Sanktionen umfassen vor allem Nummernabschaltungen, aber auch Gerichtsverfahren. Von September 2003 bis Ende 2005 wurden rd. 900 Nummern abgeschaltet und drei Verfahren eingeleitet, die alle von der BNetzA gewonnen wurden. Die Rechtsprechung auf diesem Gebiet wird allgemein als so eindeutig eingeschätzt, dass diejenigen, die Rufnummern-Spamming betreiben, kaum Widerspruch gegen die Urteile einlegen bzw. sich den Sanktionen der BNetzA beugen.

Abbildung 2-2: Missbrauch von (0)190er/(0)900er Mehrwertdiensterufnummern bei unerwünschten Massenaussendungen (2004)



insgesamt 3.703 Beschwerden eingegangen

Quelle: RegTP Jahresbericht 2004 (Stand: 31.12.2004)

[13] Vom 11.4.2005 bis 30.11.2005 wurden 23.500 Beschwerden gezählt. Eine endgültige Zählung wird für den Jahresbericht 2005 Anfang des Jahres 2006 vorgenommen.

Rufnummern-Spamming wird aber voraussichtlich kaum abnehmen, weil erst die Ergänzung der Massenaussendungen durch MWD-Rufnummern eine für die Sender höchst lukrative Einnahmequelle erschließt. Bei einer einfachen Werbemail kann die Reaktion der Empfänger stark von „keine Antwort“ bis „Vertragsabschluss mit Neukunden“ variieren und die Rückantwort selbst generiert noch keine Einnahmen beim Sender. Die Verwendung bzw. Aktivierung einer MWD-Rückrufnummer in der unerwünschten Nachricht garantiert aber, dass der Beworbene für jede Antwort an den Sender, aus welcher Motivation auch immer, zahlen muss. Eine Abschaltung der Nummern bewirkt daher häufig nur, dass neue Nummern für ähnliche Spam-Aktionen missbraucht werden. Experten bemängeln, dass z.B. die geringen Bußgelder, die die Behörde verhängen kann, keine ausreichend abschreckende Wirkung zeitigen. Die möglichen Sanktionen sind:[14]

- Abmahnungen,
- Androhung und Festsetzung von Zwangsmitteln,
- Abschaltung von Rufnummern,
- Untersagung der Rechnungslegung,
- Untersagung der Inkassierung,
- Entzug von Rufnummern,
- Widerruf oder Rücknahme von Registrierbescheiden,
- Einleitung von Bußgeldverfahren.

2.5 Zusammenfassung

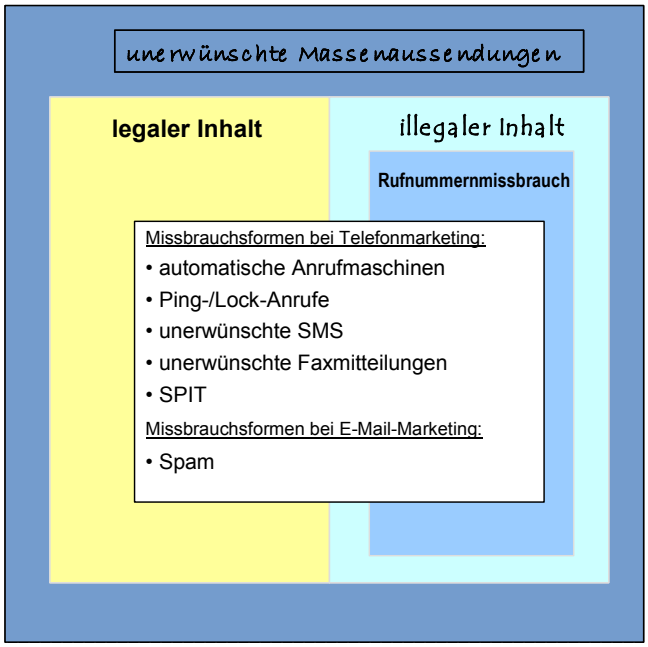
Für alle Formen kommerziell motivierter Kommunikation über elektronische Medien wird im Folgenden der gebräuchliche Begriff „unerwünschte Massenaussendungen“ verwendet. Unter Spam verstehen wir ausschließlich den Missbrauch von E-Mail-Marketing. Den in die Zuständigkeit der Bundesnetzagentur fallenden Missbrauch bezeichnen wir als Rufnummern-Spamming.

Ordnet man die genannten Formen der unerwünschten Massenaussendungen den verschiedenen Missbrauchsbereichen zu, ergibt sich folgendes Bild:

---

14 Eine aktuelle Liste der verhängten Sanktionen findet sich unter www.bundesnetzagentur.de.

Abbildung 2-3: Definition „Unerwünschte Massenaussendungen“



Quelle: WIK

3 Transaktionskosten durch Spam am Beispiel von E-Mail

3.1 Effizienzgewinne durch E-Mail

Der Telekommunikationsdienst E-Mail hat eine fast beispiellose Erfolgsgeschichte aufzuweisen. Im Zeitraum von nur einem Jahrzehnt hat sich E-Mail als eines der wichtigsten Kommunikationsmedien weltweit sowohl in der geschäftlichen wie auch der privaten Kommunikation etablieren können. Neben dem WWW hat der E-Mail-Dienst einen mindestens gleichwertigen Beitrag zum Erfolg des Internet geleistet und gilt als eine der Killerapplikationen.

Zu den ausschlaggebenden Gründen für den Erfolg von E-Mail zählen die äußerst geringen Kosten und die Schnelligkeit der Übermittlung. Auf der Grundlage der heute mehr und mehr genutzten Flatrates beim Internetzugang gehen die Grenzkosten für den E-Mail-Versand praktisch gegen Null und sind entfernungsunabhängig. Die hohe Effizienz von E-Mail ergibt sich zudem dadurch, dass ein Großteil der heutigen Informationen elektronisch verarbeitet werden und per E-Mail asynchron ohne Medienbruch verschickt und mit beliebig vielen Kommunikationspartnern geteilt werden kann. E-Mail ist ein ideales Transport- und Archivierungsmedium für umfangreiche Textdokumente, Präsentationen, Fotos und Multimediadateien. Da insbesondere im Geschäftsleben eine permanente Verbindung zum Internet besteht, sei es per PC am Arbeitsplatz oder per Mobilfunkgerät wie etwa dem E-Mail-Dienst Blackberry, erreichen E-Mails ihre Adressaten praktisch unmittelbar nach dem Versenden. Im Gegensatz zum Telefongespräch, das eine simultane Aufmerksamkeit der Kommunikationspartner erfordert, ist diese bei E-Mail nur konsekutiv erforderlich, was die Erreichbarkeit erhöht und auch die Kommunikation über Zeitzonen hinweg erleichtert.

Durch den Einsatz von E-Mail haben sich alle Arten von Koordinations- und Organisationsprozessen deutlich beschleunigt. Die Reaktionszeiten in der Kommunikation von und mit Unternehmen und Behörden haben sich in der Regel stark verkürzt, Bestellungen und Anträge werden schneller abgewickelt. Durch E-Mail hat eine Substitution traditioneller Kommunikationsdienste statt gefunden. In der geschäftlichen Kommunikation wurden die Dienste Telegramm und Telex vollständig sowie das Telefax zum Großteil substituiert oder ergänzt. Doch auch Sendungen per Briefpost und der Informationsaustausch per Telefonanruf werden heute vielfach durch E-Mails ersetzt.

Das Kommunikationsmedium E-Mail dient dank seiner hohen Effizienz nicht nur als Ersatz für andere Kommunikationsdienste, sondern ermöglicht zudem neue Formen des Informationsaustauschs, bei denen die Grenzen der Individualkommunikation aufgebrochen werden. Der E-Mail-Dienst schafft die Voraussetzungen für eine individualisierte Gruppen- und Massenkommunikation zu konkurrenzlos niedrigen Kosten und ohne Zeitverzögerung. Das Informationsmedium des Newsletters ist in seiner heutigen Ausprägung und Vielfalt nur durch E-Mail möglich. Das Direktmarketing oder der Infor-

mationsaustausch zwischen den Mitgliedern von Interessengruppen bekommt eine völlig neue Qualität. Auch innerhalb von Hierarchien können Informationen und Botschaften per E-Mail simultan an beliebig große Adressatenkreise übermittelt werden und dies vollkommen ortsunabhängig.

Die hohe Effizienz und die zusätzlichen Möglichkeiten des E-Mail-Dienstes führten nicht nur zu strukturellen Veränderungen im Kommunikationsverhalten, sondern auch zu Veränderungen von Organisations- und Produktionsstrukturen. Insbesondere wird der weitere Ausbau der internationalen Arbeitsteiligkeit forciert. Weltweit dislozierte Stufen von Wertschöpfungsketten lassen sich durch E-Mail ebenso effizient managen wie räumlich verteilte Administrationen. Die Strukturveränderungen beim Umfang und der Verortung der Arbeitsteilung haben wiederum akzelerierende Wirkung auf die Anzahl der verschickten E-Mails.

Den Vorteilen von E-Mail stehen von vornherein auch systemimmanente Nachteile entgegen. Der über das offene Internet übertragene E-Mail-Dienst wurde als Best-Effort-Dienst konzipiert und bietet weder eine absolute Verlässlichkeit, dass die E-Mails ihre Adressaten erreichen, noch Vertraulichkeit durch standardisierte Verschlüsselung. Verschlüsselungsverfahren müssen vielmehr im Nachhinein implementiert und von jedem Nutzer mit einigem Aufwand angewandt werden. Auch die Authentizität des Absenders ist ohne eine qualifizierte digitale Signatur nicht garantiert. Dem Erfolg von E-Mail haben diese Nachteile jedoch keinen Abbruch getan. Die Effizienzvorteile wurden von den Nutzern in aller Regel weit höher gewichtet als die Sicherheitsvorteile, die die zentralhierarchisch organisierte Briefpost bietet.

Nicht nur die Gesamtmenge der weltweit verschickten E-Mails hat während der letzten Jahre mit enormen Wachstumsraten zugenommen. Auch aus der Sicht eines einzelnen E-Mail-Nutzers lässt sich eine Ausweitung der Kommunikation feststellen, die in vielen Fällen dramatische Ausmaße angenommen hat. Sowohl die Anzahl der Kommunikationskontakte als auch die Kommunikationsfrequenz sind im E-Mail-Zeitalter stark angestiegen.

Das Medium E-Mail kann je nach Nutzungskontext und Kommunikationspartner für einen zwanglosen Chat genauso genutzt werden wie für einen förmlichen Geschäftsbrief. E-Mails können neben dem Hauptadressaten offen oder verdeckt an weitere Adressaten verschickt und beliebig weitergeleitet werden. Sie können zudem zu geringen Kosten beliebig lange gespeichert und noch nach Jahren mit Hilfe von Suchmaschinen ausgewertet werden. Alle diese Eigenschaften ermöglichen einerseits einen variantenreichen Umgang und eine vielfältige Nutzung dieses Mediums, führen jedoch auch gleichzeitig zu einer zunehmenden Komplexität und Intensität der Kommunikation, die vor dem Hintergrund der großen Anzahl an E-Mails, die Effizienzgewinne zum Teil wieder aufzehren, kompensieren oder sogar übersteigen kann. Zu beobachten ist mitunter sogar eine Überforderung der Nutzer, die mit einer Anpassung ihres Umgangs mit dem

Medium reagieren, um in der Informations- und Kommunikationsflut nicht den Überblick zu verlieren.

Die Kosteneffizienz des E-Mail-Dienstes, seine hohe Penetration und seine Eignung zur individualisierten Massenkommunikation bieten leider auch einen nahezu idealen Nährboden für die missbräuchliche Nutzung. Innerhalb sehr kurzer Zeit entwickelte sich Spam vom vereinzelt auftretenden Ärgernis zum bedrohlichen Massenphänomen. Die E-Mail-Nutzer müssen nun nicht nur Wege finden, mit dem steigenden Aufkommen an erwünschter Kommunikation umzugehen, sondern werden gleichzeitig auch mit einer Überflutung ihrer E-Mail-Fächer durch Spam konfrontiert.

Seit dem Aufkommen und der enormen Zunahme von Spam ist die Nutzung des an sich äußerst kostengünstigen E-Mail-Dienstes mit steigenden Kosten verbunden. Diese durch Spam verursachten Kosten belasten mehr und mehr die Kosten-Nutzen-Bilanz des E-Mail-Dienstes und stellen eine massive Belastung nicht nur für die Nutzer, sondern auch für deren Anbieter dar.

3.2 Analogie zur Transaktionskostentheorie

Charakteristisch für die durch Spam verursachten Kosten ist, dass sie weniger durch die Erzeugung bzw. Bereitstellung des Dienstes an sich, sondern im Zusammenhang mit der Nutzung des offenen Kommunikationssystems Internet entstehen. In zentral organisierten, geschlossenen Kommunikationssystemen wie z. B. dem PSTN oder der Briefpost können diese Kosten hingegen weitgehend vermieden werden, da hier Versender unerwünschter Massenaussendungen vom Betreiber oder Nutzer schnell identifiziert und weitgehend gesperrt werden können. Für geschlossene Systeme, z. B. E-Mail in geschlossenen Benutzergruppen, müssten jedoch die zahlreichen Effizienzvorteile des Internet aufgegeben werden.

Bei dieser Betrachtung liegt eine Analogie zur Transaktionskostentheorie nahe. Das theoretische Konzept der Transaktionskosten, das seinen Ursprung in der Erklärung der Entstehung und Veränderung von Unternehmungen hat und den Hauptanstoß für die Entwicklung der Neuen Institutionenökonomik lieferte, geht auf Ronald Coase[15] zurück. Coase betrachtet Markt und Unternehmungen als alternative Koordinationsmechanismen. Die unternehmensinternen Koordinationen erzeugen Organisationskosten, während marktliche Koordinationen mit (Markt-)Transaktionskosten einhergehen. Transaktionskosten sind in diesem Sinne alle Kosten, die bei der Nutzung des Marktes entstehen. Sie „lassen sich untergliedern in

- die Kosten der Anbahnung von Verträgen (Such- und Informationskosten im engen Sinne),

15 Vgl. Coase (1937).

- die Kosten des Abschlusses von Verträgen (Verhandlungs- und Entscheidungskosten),

- die Kosten der Überwachung und Durchsetzung vertraglicher Leistungspflichten."[16]

Nach der Transaktionskostentheorie erfolgt die Entscheidung darüber, welche wirtschaftlichen Aktivitäten auf Märkten über den Preismechanismus und welche innerhalb von Unternehmungen über Anweisungen koordiniert werden nach dem Prinzip der marginalen Substitution („make or buy"). Unternehmen übernehmen so viele Transaktionen, „bis ihre Organisationskosten für die Einbeziehung einer weiteren Transaktion den Kosten der Abwicklung dieser Transaktion über den Markt oder den Kosten ihrer Organisation in einer anderen Unternehmung entsprechen."[17]

In der Analogie mit der Transaktionskostentheorie ist das Internet als offenes, dezentral organisiertes Kommunikationsnetz, in dem Datenpakete durch Standardprotokolle übermittelt werden, mit dem Markt zu vergleichen, dem ebenso eine offene, dezentrale Organisation zu Grunde liegt und auf dem die Produktionsaktivitäten durch den Preismechanismus koordiniert werden. Beim Gegenstück zum Markt, der Unternehmung, werden die Produktionsaktivitäten mittels Anordnungen zentral gesteuert und sind vergleichbar mit geschlossenen, zentral organisierten elektronischen Kommunikationssystemen.

So wie hohe Kosten einer Markttransaktion (beispielsweise hohe Überwachungs- oder Durchsetzungskosten) das Zustandekommen eines Handels von vorneherein verhindern können, bewirken hohe Kosten durch Spam möglicherweise eine Verminderung der Kommunikation über E-Mail und führen zu Ausweichreaktionen in Richtung auf jene Kommunikationsmittel, die aufgrund ihrer Organisationsform kaum unerwünschte Massenaussendungen provozieren.

Beispiel für ein zentral gesteuertes elektronisches Kommunikationssystem sind SMS und MMS über Mobilfunk. Das Problem unerwünschter Massenversendungen kann durch die zentrale Überwachung des Netzbetreibers relativ klein gehalten werden. Die Identifizierung des Absenders stellt kein Problem dar, so dass Massenversender rasch gesperrt werden können.[18] Statt der Transaktionskosten durch Spam fallen beim SMS-Versand allerdings dramatisch höhere Übertragungsentgelte an und es bestehen weitere Nutzungsrestriktionen im Vergleich zum E-Mail-Dienst. So ist der SMS und MMS-Austausch beispielsweise nicht mit allen ausländischen Mobilfunknetzen möglich und es bestehen Größenbeschränkungen für die Texte und die Anhänge.

---

16 Vgl. Richter/Furubotn (1996), S. 51.
17 Vgl. Bössmann (1981), S. 670.
18 Dies gilt natürlich nur, solange der SMS-Dienst nicht für den Empfang von E-Mail-Nachrichten geöffnet wird.

3.3 Transaktionskosten durch Spamming

Im Rahmen einer qualitativen Analyse sind mehrere Kategorien von Transaktionskosten durch Spamming zu unterscheiden. Die Transaktionskosten auf Seiten der Nachfrager und Nutzer von E-Mail-Diensten bestehen unter anderem aus

- den Übertragungskosten für Spam,
- der Zeit für die manuelle Selektion von Spam,
- dem Risiko, erwünschte eingehende E-Mails versehentlich als Spam zu löschen, bzw. der Ungewissheit, ob versendete E-Mails angesichts der hohen Anzahl an Spam vom Adressaten wahrgenommen werden,
- dem Risiko einer Infizierung mit Malware (Würmer, Trojaner, Viren) und
- nicht zuletzt aus einem generellen Vertrauensverlust.

Auf Seiten der ISP fallen insbesondere Transaktionskosten durch Spam an durch

- das höhere E-Mail-Verkehrsaufkommen,
- einen größeren Speicherbedarf,
- die entgangenen Umsätze durch niedrigere Nutzungsraten in Folge von Spam und
- schließlich das Risiko, dass ohne geeignete Gegenmaßnahmen das E-Mail-System langfristig unbrauchbar wird und als Geschäftsgrundlage wegfällt.

Wie bei den Transaktionskosten, die bei einer Marktkoordination anfallen, lassen sich auch die Transaktionskosten durch Spamming auf Grund enormer Bewertungs- und Zurechnungsschwierigkeiten nur schwer quantifizieren.[19]

Anbieter wie auch Nutzer von E-Mail haben gleichermaßen ein großes Interesse daran, die Funktionalität und Effizienz von E-Mail aufrechtzuerhalten und die Transaktionskosten durch Spam zu minimieren. Sie ergreifen daher Maßnahmen, die Spam reduzieren sollen, die jedoch auch selbst Kosten verursachen. Sie tun dies in der Erwartung, dass durch die Abwehrmaßnahmen die Transaktionskosten durch Spam dem Betrag nach deutlich stärker sinken als dass diese Maßnahmen neue Kosten verursachen. Soweit sich die Akteure ökonomisch rational verhalten, kommen Gegenmaßnahmen, deren Kosten höher sind als die Transaktionskosten durch Spam, nicht zum Einsatz.

Zu den Kosten für Gegenmaßnahmen, die bei den E-Mail-Nutzern anfallen zählen,

- die Kosten für die Einrichtung und Pflege von Spam-Filtern im E-Mail-Client,

---

19 Vgl. Richter/Furubotn (1996), S. 56 ff

- insbesondere bei Business-Usern mit größeren Firmennetzen die Kosten für Soft- und Hardware, die in Zusammenarbeit mit dem Mailserver Spam aussortiert sowie
- Kosten, die dadurch entstehen, dass erwünschte E-Mails durch die Gegenmaßnahmen fälschlicherweise als Spam klassifiziert und aussortiert werden.

Bei den Anbietern von E-Mail-Diensten fallen insbesondere Kosten an für

- die Entwicklung, Einrichtung und permanente Pflege von Spam-Filtern sowie sonstiger technischer Maßnahmen,
- die Organisation von anbieterübergreifenden Arbeitsgruppen und der Ausarbeitung von Strategien gegen Spam,
- die rechtliche Absicherung im Zusammenhang mit dem Einsatz von Gegenmaßnahmen und
- die Einleitung rechtlicher Maßnahmen gegen Spam-Versender.

4 Geschäftsmodelle für Massenaussendungen

Zur Analyse des Phänomens der unerwünschten Massenaussendungen ist es notwendig, die ökonomischen Rationalitäten auf Seiten der Versender und ihre darauf aufbauenden Geschäftsmodelle zu untersuchen. Wie andere wirtschaftliche Aktivitäten auch, basieren die Massenaussendungen zur Gewinnung von Kunden für kommerzielle Angebote auf Kosten-Nutzen-Rechnungen.

Die wichtigste Kennziffer einer solchen Kalkulation, sowohl für seriöse wie auch für unerwünschte Massenaussendungen, ist der Break-Even-Point (BEP) einer Werbeaussendung.[20] Der BEP bezeichnet die zur Kostendeckung erforderliche Rücklaufquote einer Massenaussendung, d.h. die abgeschlossenen Geschäfte im Verhältnis zur Gesamtzahl der versendeten Werbebriefe. Liegt die Rücklaufquote oberhalb des BEP, so ist die Massenaussendung profitabel.

Der BEP errechnet sich durch den Quotienten aus Werbekosten und Auftragsspanne. Die Auftragsspanne ist dabei die Differenz aus dem Verkaufspreis und den Stückkosten des Anbieters. Je geringer die Kosten der Massenaussendung bzw. je größer die Auftragsspanne, umso kleiner ist die erforderliche Rücklaufquote:

$$\frac{Kosten\ je\ Aussendung}{Auftragsspanne\ je\ Auftrag} = BEP$$

Massenaussendungen per Briefpost beinhalten relativ hohe Kosten für die Herstellung und den Versand des Werbebriefs. Der Deutsche Direktmarketing Verband (DDV) kalkuliert in Beispielrechnungen für Massenaussendungen im Bereich Business to Consumer bei einer Gesamtauflage von 50.000 Stück ca. 0,61 € für Standardmailings und 1,11 € für hochwertige Mailings je Aussendung (vgl. Tabelle 4-1).

20 Vgl. Hölscher (1991), S. 538.

Tabelle 4-1: Kosten für postalischen Massenversand (Beispiel Standard- und Hochwertiges Mailing)

Arbeitsgänge*	Standardmailing	Hochwertiges Mailing
Druck und Weiterverarbeitung von Versandhülle, personalisierter Brief, personalisierter Responseschein, Antworthülle, (Prospekt groß, Prospekt klein)	90 €	225 €
Adressieren, Personalisieren, Schneiden, Falzen, Kuvertieren, Frankieren, Postaufliefern	65 €	75 €
EDV-Arbeiten, Fremdadressen konvertieren und analysieren, postalisch prüfen, Dublettenabgleich, inkl. Robinsonliste, (Umzugs- und Negativabgleich), Portooptimierung	45 €	140 €
(Hochwertige) Fremdadressen zur einmaligen Nutzung	160 €	200 €
Porto Infopost	250 €	470 €
Gesamtkosten pro 1.000 Aussendungen bei Gesamtauflage von 50.000	**610 €**	**1.110 €**

* Arbeitsgänge in Klammern wurden nur für hochwertiges Mailing kalkuliert.

Quelle: DDV (2004), S. 22.

Angenommen, pro erfolgreichem Vertragsabschluss verbleibt dem Anbieter eine Auftragsspanne von 50 €, so ergeben sich folgende BEP für

Standardmailing: $\frac{0{,}61\,€}{50\,€} = 0{,}0122$

hochwertiges Mailing: $\frac{1{,}11\,€}{50\,€} = 0{,}0222$

Im Falle des Standardmailings müssen somit mindestens 1,22% und beim hochwertigen Mailing 2,22% der angeschriebenen Adressaten das beworbene Angebot nachfragen, damit die Gewinnzone erreicht wird.

Die Entscheidung darüber, wie aufwändig Massenaussendungen gestaltet werden, lässt sich mit Hilfe der Werbewirkungsforschung treffen. Nach dem klassischen „AIDA-Modell“ der Werbewirkung muss eine Direktwerbung beim Adressaten Aufmerksamkeit (Attention) erzeugen, Interesse (Interest) wecken, den Wunsch (Desire) nach dem beworbenen Angebot generieren und schließlich eine Kaufhandlung (Action) auslösen.[21] Die Versender herkömmlicher Massenaussendungen wenden relativ viele Ressourcen auf, um durch zielgruppenorientierte Ansprache und Gestaltung die Werbewirkung und die Effizienz der Massenaussendung zu steigern. Vorraussetzung hierfür sind zielgruppengenaue Adressensätze, die entsprechend teuer gehandelt werden.

21 Vgl. Kroll (1991), S. 762.

Im Unterschied zu diesem klassischen Geschäftsmodell der Direktwerbung verfolgen die Absender von elektronischen Massenaussendungen ein gänzlich anderes Geschäftsmodell. In der Herstellung fallen dramatisch geringere Kosten an, da Material-, Druck- oder Weiterverarbeitungskosten entfallen. Sobald der Werbeinhalt elektronisch erstellt wurde, kann er ohne weitere Kosten beliebig oft dupliziert werden. Der Versand von Spam erfolgt daraufhin zu marginalen Kosten je Exemplar.

Da die Stückkosten für Erstellung und Versand bei Spam nahe bei Null liegen, ist es für die Versender dieser E-Mails rational, möglichst allen verfügbaren E-Mail-Adressen ein Exemplar der Werbebotschaft zu schicken, unabhängig davon, ob die Adressaten zur primären Zielgruppe für das beworbene Angebot zählen oder nicht. Um die Kosten für die Gewinnung von Adressen gering zu halten, werden Automaten eingesetzt, die das World Wide Web nach E-Mail-Adressen durchsuchen sowie Adressen aus beliebigen Namenskomponenten generieren. Während beim klassischen Werbebrief viel Aufwand betrieben wird, um falsche Adressen zu vermeiden und damit Kosten zu sparen, spielt es auf Grund der Kostensituation beim Spamming keine Rolle, dass ein Großteil der eingesetzten Adressen ungültig ist.

Für eine Beispielsrechnung sollen die Gesamtkosten für die Erstellung eines Spam-Mailings und seiner Versendung an 10 Mio. Empfänger mit 1.000 € angenommen werden. Bei einer hypothetischen Auftragsspanne von 50 € ergibt sich ein BEP von 0,002‰.

$$\frac{0{,}0001\,€}{50\,€} = 0{,}000002$$

Das bedeutet, dass die Gewinnzone für den Spamversender bereits erreicht wird, wenn mehr als 2 von 1.000.000 Adressaten das Angebot nachfragen.

Um die Werbewirkung ihrer Massenaussendungen zu erhöhen, greifen Spamversender vielmals auf reißerische oder persönlich vertraulich klingende Betreffzeilen oder auch pornografische Bilder zurück. Zudem handelt es sich bei den angebotenen Produkten oder Dienstleistungen zum Großteil um erotische Angebote, gefälschte Ware zu vermeintlich sensationellen Preisen oder um sonstige illegale Produkte wie Medikamente, Software oder Kreditangebote.

Im Unterschied zu den seriösen Direktwerbern beinhaltet das Geschäftsmodell von Spam-Versendern nicht die Pflege eines Markennamens zum Aufbau von Reputation. Ganz im Gegenteil verschleiern diese meist ihre Identität, um einer juristischen Verfolgung auf Grund der Versendung unerwünschter Massenaussendungen, der Anwendung unseriöser Geschäftspraktiken oder dem Vertrieb illegaler Produkte zu entgehen.

Auch wenn die Direktwerbung per E-Mail durch die Spam-Versender einen erheblichen Imageschaden genommen hat, so bleibt dieses kostengünstige Medium auch für seriö-

se Anbieter eine attraktive Alternative zum Postversand von Werbebriefen. Angesichts des massenhaften Missbrauchs durch Spam-Versender spielt bei seriösen Unternehmen die Zielgenauigkeit ihrer Massenaussendungen eine umso größere Rolle. Entsprechend müssen Ressourcen für die sorgfältige Adressenpflege aufgewendet werden und es bedarf Kooperationen mit den ISP, um erwünschte Massenaussendungen von Spam zu unterscheiden und nicht auszusortieren.

5 Missbrauch durch unerwünschte Massenaussendungen

5.1 Anteil des Spam am E-Mail-Aufkommen und Schätzungen über Schäden

E-Mail hat sich als universelles Kommunikationsmittel weltweit durchgesetzt. Die Menge der versendeten E-Mails hat in den letzten fünf Jahren mehr als verzehnfacht (vgl. Tabelle 5-1). Schätzungen gehen aktuell von über 50 Mrd. E-Mails pro Tag weltweit aus.

Tabelle 5-1: Entwicklung des E-Mail Aufkommens seit 1999 (Mrd. E-Mails pro Tag weltweit)

Jahr	E-Mails pro Tag
1999	5. 000 000 000
2000	10. 000 000 000
2002	31. 000 000 000
2006 geschätzt	60. 000 000 000

Quelle: IDC

Auch wenn die herkömmliche Briefpost durch E-Mail nicht vollständig ersetzt wurde, sind erhebliche Substitutionseffekte eingetreten. Sowohl in der Geschäfts- als auch in der Privatkommunikation ist E-Mail heute das vorherrschende Kommunikationsmedium, dessen Effektivität durch Spam jedoch erheblich beeinträchtigt wird.

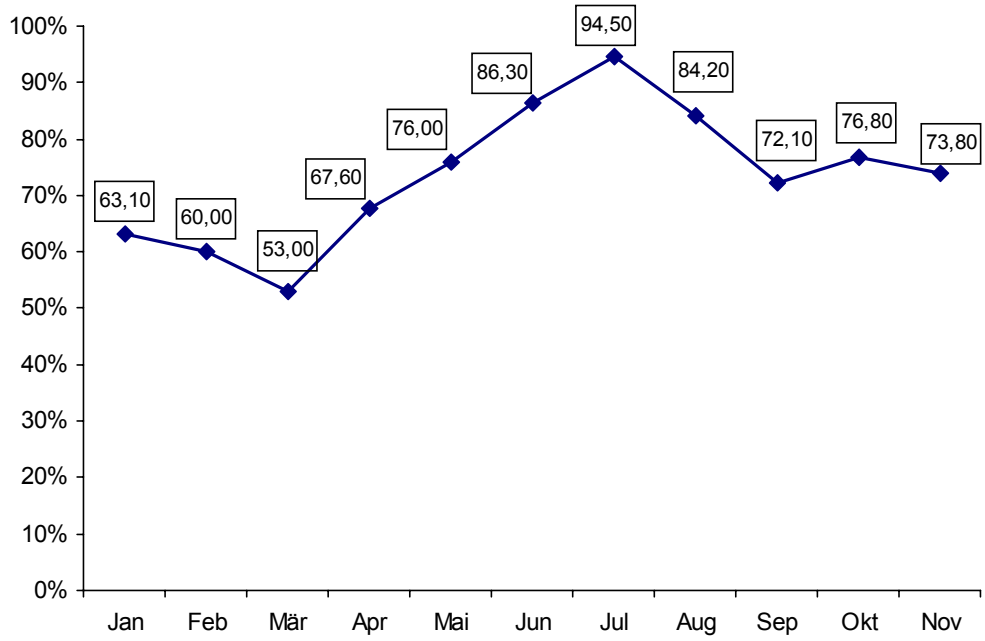
Der Anteil von Spam an den heute versandten E-Mails lässt sich empirisch nicht exakt bestimmen. ISP oder auch Filtertechnologie-Hersteller bemühen sich jedoch, durch Messungen den hohen Anteil von Spam zu belegen und kommen durch Stichproben zu validen Schätzungen über das weltweite Spam-Aufkommen.

Das New Yorker Unternehmen MessageLabs, ein Anbieter von Messaging-Security- und Management-Services für Unternehmen, führt regelmäßig detaillierte Messungen durch und kam für das Jahr 2004 zu dem Schluss, dass es sich bei rd. 74 Prozent aller E-Mails um Spam handelte. Jede 1,4 E-Mail war somit „Datenmüll“ für den Empfänger.[22] Für das Jahr 2005 zeichnet sich noch keine Trendwende ab.

---

22 Es wurden 12,6 Mrd. E-Mails gescannt. 9,2 Mrd., d.h. 73,2% (jede 1,4 E-Mail) war Spam, vgl. Message Labs Intelligence Jahresbericht E-Mail-Sicherheit 2004, www.messagelabs.com).

Abbildung 5-1: Entwicklung des Spam-Anteils am E-Mail Aufkommen in 2004 (in Prozent)



Quelle: Message Labs 2004

Auch andere Schätzungen, z.B. von IDC oder Datamonitor, nennen einen Anteil von 70 bis 80 Prozent Spam. Für Deutschland bedeutet dies, dass ca. 500 Mio. Spam-Mails pro Woche an deutsche User versandt werden (Schätzung des VZBV) und dadurch Kosten in Milliardenhöhe entstehen. Die Studie „The global economic impact of Spam 2005“ von Ferris Research schätzt sie auf 4,5 Mrd. US-Dollar jährlich.

Der Verbraucherverband VZBV, der eine Beschwerde-Hotline für private Nutzer betreibt, erhält zurzeit täglich 7.000 bis 8.000 Beschwerden über Spam. Vermutlich dürfte diese Anzahl noch steigen, je bekannter diese Sammelstelle wird. Seit Einrichtung der Hotline im Frühjahr 2005 sind insgesamt 0,5 Mio. Beschwerden eingegangen. Der Verband geht in erster Linie Spam aus Deutschland nach. Mittels manueller Sortierung können ca. 15 bis 20 Prozent als aus Deutschland stammend identifiziert werden. In etwa der Hälfte der Fälle handelt es sich um Phishing-Betrug. Der Inhalt des übrigen Spam besteht zu einem überwiegenden Teil aus Medikamenten-Werbung.

Der deutsche Spam wird an den Eco-Verband weitergeleitet, der eine ladungsfähige Anschrift identifiziert. Es wird insbesondere versucht, den Geschäftsführer des spammenden Unternehmens ausfindig zu machen. In einem ersten Schritt werden die Betreffenden zur Unterlassung aufgefordert. Dies ist von VZBV und Eco aus bisher in Fällen

geschehen. In einem zweiten Schritt wird ggf. eine einstweilige Verfügung veranlasst bzw. eine Klage angestrengt.[23]

Die höchsten Einzelschäden, insbesondere für private Nutzer, entstehen durch Rufnummernmissbrauch und Phishing. Rufnummern-Spamming verursacht durch betrügerische Mehrwertdiensterufnummern oder andere Rückrufnummern nach Schätzungen des Bundeskriminalamtes ca. 30 bis 250 Euro Schaden pro Fall, die sich dann auf einer Telefonrechnung häufig zu Summen von mehreren Tausend Euro addieren. In Einzelfällen sind Personen um 0,75 Mio. Euro durch Dialer geschädigt worden. Schäden durch Phishing werden in Deutschland auf etwa 4,5 Mio. Euro pro Jahr beziffert. Für einzelne Personen kann der Schaden erheblich sein, für Finanzdienstleister dagegen dürfte der Imageverlust und die steigende Skepsis der Kunden gegenüber der Sicherheit von Online-Banking im Vergleich zu dem direkten finanziellen Schaden weitaus gravierender ausfallen.

5.2 Schadenskategorie: Verlust von Verlässlichkeit und Integrität

Die Versendung von unerwünschten Massen-E-Mails verursacht für die Nutzer von Telekommunikationsnetzen und –diensten Schäden, die zum Teil weit über Belästigungen hinausgehen. Es steht zu befürchten, dass die Funktionalität von elektronischen Kommunikationsmedien durch unerwünschte Massen-E-Mails insgesamt in mehrfacher Hinsicht leidet, je häufiger Schäden wie etwa der Verlust von Verlässlichkeit und Integrität auftreten.

Wenn fundamentale Sicherheitsfunktionen verloren gehen, kann schließlich auch die Akzeptanz und Nutzung des E-Mail-Dienstes leiden, denn die Sicherstellung von **Verlässlichkeit**[24] elektronischer Kommunikation im Sinne eines Ausschlusses von Manipulation und Schäden stellt ein primäres Ziel für nachhaltig erfolgreiche Anwendungen dar.

Bei unerwünschten Massenaussendungen sind vor allem die Schutzziele **Integrität** und **Verfügbarkeit** bedroht. **Integrität** bezeichnet die Unversehrtheit von Daten, indem die Informationen inhaltlich korrekt sind und beworbene Dienstleistungen verbindlich und vollständig erbracht werden. Integritätsverletzungen können durch Manipulation oder Sabotage auftreten. Integrität ist sowohl im Hinblick auf die Inhalte von Kommunikation als auch auf den Absender bedeutsam.

Die **Verfügbarkeit** von Daten, d.h. die Funktionabilität von Netzen, Diensten und IT-Hard- und Software, ist durch unerwünschte Massenaussendungen ebenfalls weniger

---

23 Öffentliche Statistiken liegen dazu noch nicht vor.

24 Zur Definition der folgenden Grundbegriffe der IT-Sicherheit vgl. Kersten, H. (1995), insbes. S. 62, 76, 102.

zuverlässig gewährleistet. Durch die Verbreitung von Malware (Viren, Würmern, Trojanern etc.) mittels Spam können Ausfallzeiten auftreten und Daten verloren gehen oder beschädigt werden. Die höchste Stufe des Missbrauchs stellen in diesem Fall Denial of Service-Attacken dar, die durch die Malware induziert werden können.

5.2.1 Aussenden schädlicher Inhalte: Dialer

Anwählprogramme (Dialer) sind Software-Programme (.exe-Dateien), die auf einem Rechner eine Internetverbindung herstellen. Nach der Installation wählt sich das Programm mit Hilfe einer MWD-Rufnummer in das Netz ein. Durch den steigenden Missbrauch dieser Programme in den letzten Jahren ist in der öffentlichen Diskussion in den Hintergrund getreten, dass diese Tools prinzipiell wünschenswert sind, da sie die einfache Realisierung des Inkasso von kostenpflichtigen Downloads und Informationsangeboten im Internet über die Rechnung des jeweiligen Teilnehmernetzbetreibers ermöglichen.

Zunehmend werden Anwählprogramme dazu genutzt, die Verbraucher über die tatsächlichen Kosten zu täuschen. Dadurch ist vor allem die Integrität der Kommunikationssysteme bedroht. Die Folgen sind ein Akzeptanzverlust in Bezug auf kostenpflichtige Mehrwertdienste im Internet.

Der Schaden entsteht u.a. dadurch, dass Intransparenz über die Kosten einer Dialer-Verbindung besteht bzw. unbemerkt ein Dialer installiert wird und zusätzlich eine Verschleierung der Anbieteradresse vorgenommen wird:

- Technische Risiken: Dialer installieren sich selbst und wählen sich ein (Auto-Dialer), werden dann zur Standardverbindung bzw. lassen sich kaum wieder entfernen.
- Kostenintransparenz: Dialer bzw. Inhalte werden mit Begriffen wie „kostenloses Download“ oder „kostenloses Zugangstool“ etc. beworben. Werden Kostenangaben gemacht, sind sie so dargestellt, dass der Nutzer über die tatsächlichen (Gesamt-)Kosten im Unklaren gelassen wird.
- Verschleierung der Anbieteridentität: Der Anbieter macht keine oder falsche Angaben, so dass es dem Nutzer schwer fällt, seine zivilrechtlichen Ansprüche geltend zu machen.
- Nutzung von Rufnummern zur Einwahl: In der Regel werden MWD-Rufnummern für Dialer verwendet. Unseriöse Anbieter weichen jedoch aufgrund der zunehmenden Kontrollen mehr und mehr auf ausländische Telefonnummern, Satellitennummern oder andere Festnetznummern zurück (vgl. Tabelle 5-2); z. B. werden die Vorwahlen 0192, 0193, 0137, 01805 genutzt oder ein Verbindungsnetzbetreiber-Vorwahl wie z. B. 010xy bzw. 0100yy vorgeschaltet, um eine Auslandsnummer, angezeigt durch Präfix 00 zu verschleiern).

Illegale Dialer mit Auslands- oder Satelliten-Rufnummern

In Deutschland dürfen Dialer mit Verfügung Nr. 38/2003 der BNetzA nur noch in der Rufnummerngasse (0)900 9 (+ 7stellige Tn-Rufnr.) betrieben werden. Unseriöse Anbieter nutzen daher für ihre Aktivitäten zunehmend Auslands- oder Satellitenrufnummern. Die Angebote sind breit gestreut und beschränken sich nicht auf Erotik, sondern umfassen auch „harmlose“ Kochrezepte-Sites oder Hausaufgabenhilfen.

Die Einwahl erfolgt unbemerkt z. B. über das Windows-Programm ActiveX. In Rechnung gestellt werden bei Satellitenverbindungen etwa 3 Euro pro Minute. Nach einer automatischen Trennung nach 30 bis 40 Minuten summieren sich so zweistellige Euro-Beträge auf der Telefonrechnung des Nutzers.

Tabelle 5-2: Bekannte illegale Dialer mit Auslands- oder Satelliten-Rufnummern

Länderkennziffer	Land
00 232	Sierra Leone
00 239	Sao Tome und Principe
00 245	Guinea Bissau
00 246	Diego Garcia (Tschagosinseln)
00 269	Komoren
00 674	Nauru
00 677	Salomonen
00 681	Wallis und Futuna
00 682	Cook Inseln
00 686	Kiribati
00 688	Tuvalu
00 690	Tokelau
00 37184	Lettland
00 3725	Estland mit Zuschlag
00 3727	Estland
00 44870	Großbritannien mit Zuschlag
00 642	Neuseeland mit Zuschlag
00 6723	Norfolkinseln
00 675	Papua Neuguinea

00 679	Fidschi
00 683	Niue
00 685	Samoa
Kennziffer	**Satellit**
00 87 032	Inmarsat (B)
00 87 132	Inmarsat (B)
00 88 213	EMSAT
00 88 216	Thuraya

Quelle: BSI

5.2.2 Aussendung anstößiger, beleidigender oder verbotener Inhalte

Die Versendung von Inhalten, die die Empfänger schockieren oder beleidigen, kann zu einem Verlust der Integrität elektronischer Kommunikationsinhalte in seiner Gesamtheit beitragen. Je mehr E-Mails mit diesen Inhalten versandt werden, umso misstrauischer können Nutzer in Bezug auf Werbe-Mails und Internet-Dienstleistungen insgesamt werden.

Es geht bei dieser Form von Spam in der Regel nicht um die Verbreitung von Inhalten als solche, sondern um Werbung für Inhalte, die entweder für bestimmte Altersgruppen (Jugendschutz) oder generell verboten sind. Teilweise können diese Texte und Bilder auch gegen religiöse oder kulturelle Normen und Werte verstoßen. In diesem Zusammenhang ist besonders problematisch, dass die Spam-Mails in der ganzen Welt versandt werden und die Inhalte in unterschiedlichem Ausmaß gegen bestehende Gesetze verstoßen. Dies hat Folgen für die Spam-Bekämpfung: Es geht sowohl um die generelle Verminderung der unerwünschten elektronischen Post als auch um die Durchsetzung nationaler Regelungen.

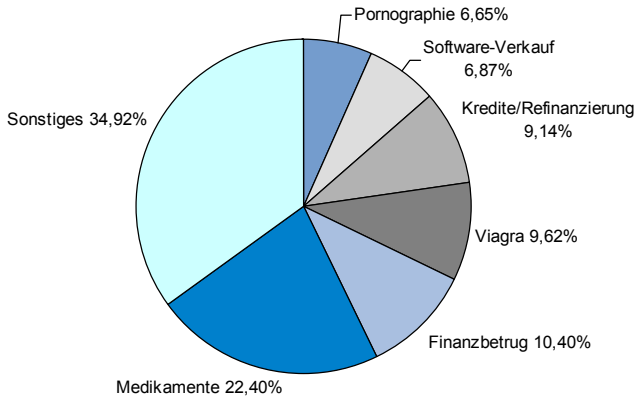
Pornographie und Werbung für Medikamente, insbesondere Viagra, machen einen erheblichen Teil des Spam aus: Insgesamt rd. 40 Prozent der unerwünschten E-Mails entfallen hierauf.[25] Der Anteil von Werbung für Medikamentenverkauf beläuft sich Erhebungen des Anti-Spam-Software Herstellers Commtouch auf 22,4% des gesamten Spam-Aufkommens. Hinzu kommen 9,62% des Spam allein für Viagra-Werbung (vgl. Abbildung 5-2).

Besonders riskant erscheint, dass auch rezeptpflichtige Medikamente oder auch Arzneien, deren Wirkung umstritten ist, stark beworben oder auch gefälschte Mittel in Um-

25 Commtouch (2005): Commtouch Reports March Spam Trends: Sharp Rise In Financial-Fraud Related Spam, Press Release 12.04.2005

lauf gebracht werden. In manchen Ländern ist der Online-Medikamentenverkauf außerdem grundsätzlich verboten bzw. wie in Deutschland nur unter strengen Regularien gestattet (z. B. Online-Beratung nur durch Apotheker).

Abbildung 5-2: Anteil von Medikamentenwerbung am Spam-Aufkommen



Medikamente	22,40 %
Finanzbetrug	10,40 %
Viagra	9,62 %
Kredite / Refinanzierung	9,14 %
Software-Verkauf	6,87 %
Pornographie	6,65 %

wik

Quelle: Commtouch (2005)

Nach einer Studie der US-amerikanischen Federal Trade Commission (FTC) enthalten zwei Drittel aller Spam-Mails offensichtlich gefälschte Informationen in der Absender- oder Betreffzeile oder sind im Text als Spam leicht erkennbar.[26]

5.2.3 Betrugsversuche

Bei Internet-Betrug handelt es sich oftmals um bekannte Vorgehensweisen und Inhalte, die jedoch durch die kostengünstige elektronische Verteilung von Nachrichten oder die elektronischen Möglichkeiten der Kontaktaufnahme weltweite Bedeutung erlangt haben und zu einem Massenphänomen geworden sind. Auch diese Art von Spam bedroht die Integrität des elektronischen Kommunikationssystems.

Bei 63,5% aller in den USA gemeldeten Betrugsversuche fand die Kontaktaufnahme über E-Mail statt.[27] Es ist davon auszugehen, dass es sich dabei um Spam handelt, der

26 Vgl. FTC (2003).

ziellos an alle Internet-Nutzer versandt wird. Inwieweit Nutzer geschädigt werden, hängt nicht zuletzt von Sprachkenntnissen (viele der Offerten sind in englischer Sprache verfasst) sowie vom Bildungsstand oder auch von der eigenen finanziellen Situation und der persönlichen „Gier nach Geld“ ab, die dazu führen kann, auch unwahrscheinlichsten Renditeversprechungen zu glauben. Scham hält nach Vermutungen von Polizeiexperten viele Geschädigte davon ab, die Vorfälle zu melden, so dass von einer hohen Dunkelziffer ausgegangen werden muss.

5.2.3.1 Social Engineering: Phishing-Mails

Phishing-Mails[28] zu versenden ist eine häufige Variante des Identitätsdiebstahls durch Social Engineering. Ziel des Social Engineering ist es, durch Vorspiegelung einer seriösen Umgebung (Nutzung des Layouts einer bekannte Website, Anruf eines „Bankmitarbeiters“ u.ä.) an die Identifikationsdaten eines Nutzers zu gelangen und diese für eine Straftat zu verwenden. Viele Banken, u.a. die Postbank, die Deutsche Bank und die Volksbanken Raiffeisenbanken hatten bereits mit Phishing-Betrug zu kämpfen.

Beim Phishing werden Spam-E-Mails dazu benutzt, Links zu Finanzinstitutionen zu versenden, z. B. Kreditkartenorganisationen, Banken, Electronic Wallet Services. Klickt der Empfänger den HTML-Link an, der den Quelltext eines ganz anderen Links verbirgt, wird er zu einer täuschend echten Website weitergeleitet und aufgefordert, die Zugangskennung zu seinem Konto (PIN/TAN) einzugeben. Die Phishing-Betrüger nutzen dabei entweder Internetadressen, die sich nur geringfügig von denen der bekannten unterscheiden (z. B. www.bank.net statt www.bank.de) oder sie fälschen die Adressleiste des Browsers mit einem Java-Script.

Die Betrüger nutzen die Daten dann dazu, um Konten zu belasten oder auch, um nur einen unauffälligen Betrag abzubuchen. Durch die Verletzung der Integrität der Absenderadresse kann beim Kunden über den finanziellen Schaden hinaus ein nachhaltiger Vertrauensverlust in das zumeist ohne Signatur oder Verschlüsselung verwendete E-Mail-System entstehen. Dieses Risiko besteht auch für die große Masse der Nicht-Kunden, die über die Medien von diesen Problemen Kenntnis nehmen und schadet somit der gesamten Finanzdienstleistungsbranche.

Angriffsversuche hat es in den USA, aber auch in Deutschland in hohem Ausmaß gegeben. Das BKA warnt seit Frühjahr 2004[29] im Internet vor Phishing-Betrug. Auch die Postbank macht ihre Kunden auf diesen Trick im Zusammenhang mit Spam an Post-

---

27 IC3 2004 Internet Fraud - Crime Report January 1, 2004 - December 31, 2004, S. 14. In 23,5% der Fälle fand die Kontaktaufnahme über Websites statt. Telefon (7%), Chatrooms (0,7%) sowie Fax (0,2%) und andere Methoden spielen nur eine untergeordnete Rolle.

28 Phishing ist ein Kunstwort des Computer-Slang und bedeutet soviel wie „Fischen nach Passwörtern“.

29 Vgl. BKA, Pressemitteilung v. 19.03.2004 Bundeskriminalamt warnt vor Kreditkartenbetrügern.

bank-Kunden seit Sommer 2004 aufmerksam. Aktuell wurde Mitte April 2005 wieder ein großangelegter Betrugsversuch bekannt (vgl. Abbildung 5-3).[30]

Abbildung 5-3: Beispiel für Phishing-Mails

From: "PostBank" security@postbank.de

To: "PostBank Kunde"

Sehr geehrter Kunde,

Da es viele Betrugsfaelle mit den Konten von unseren Bankkunden zustande gekommen sind, bitten wir Sie, eine neue TAB-Kodesabsicherung zu benutzen, um die Sperrung von Ihrem Konto zu vermeiden.

Die TAN-Absicherung besteht darin:

Sie tasten zwei TAN-Nummern in die elektronische Form ein und streichen bei Ihnen diese Nummern aus.
Fuer den Fall, dass der Misstaeter Ihre TAN-Codes abfaengt und sie zu benutzen versucht, so wird Ihr Konto bis zur Klaerung der Sachlage gesperrt. Danach benutzen Sie alle Nummern, ausser diesen 2, der Reihe nach weiter.

Um den Abgang der Mittel von Ihrem Konto zu vermeiden, bitten wir alle, die Form auszufuellen, da wir die Mittel nicht vergueten, die zufolge dem Diebstahl von Ihrem Online-Zugriff zu unserem Bankkonto verlorengegangen sind.

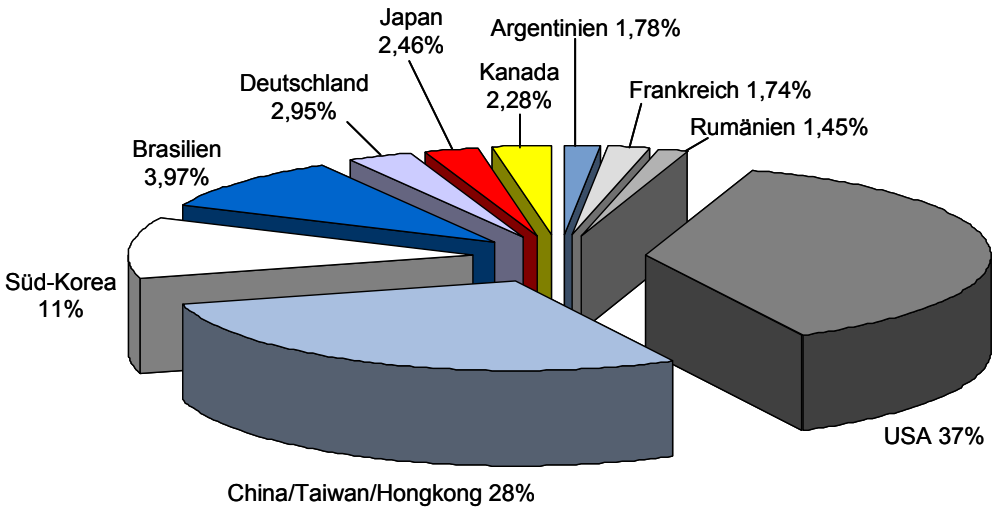
Sie koennen die Form bei ausfuellen http://.....

Quelle: Postbank

Die international orientierte US-Industrieorganisation „Anti-Phishing Working Group – APWG“ berichtet von 2.625 gemeldeten Phising-Sites im Februar 2005.[31] Das bedeutet einen durchschnittlichen Zuwachs von 26% seit Juli 2004. Im Februar wurden an APWG in diesem Zusammenhang 13.141 verschiedene Formen von neuen Spam-E-Mails gemeldet. Dies deutet auf Millionen von Spam-E-Mails allein durch diese Betrugsversuche hin. Die Identifikation der Phisher gestaltet sich schwierig, weil die meisten Websites außerhalb Deutschlands gehostet werden (vgl. Abbildung 5-4). Entsprechend aufwändig ist auch die Verfolgung der Verursacher.

30 Vgl. die Informationen auf der Website der Postbank www.postbank.de.
31 APWG - Anti-Phishing Working Group (2005): Phishing Activity Trends Report, February 2005.

Abbildung 5-4: Anteil der Phishing-Hosts im internationalen Vergleich



Quelle: APWG February 2005 (www.antiphishing.org)

Hauptsächlich betroffene Branche ist die der Finanzdienstleistungen (78% aller Phishing-Websites), erst mit weitem Abstand folgen Internet Service Provision (13%) sowie Einzelhandel (3%). Auf weitere Branchen entfallen 6% der Sites.

5.2.3.2 Vorkasse-Betrug: „Nigeria Connection“

Betrügerische „Nigeria-Nepp“ E-Mails[32] versuchen typischerweise den Empfänger davon zu überzeugen, dass eine mit ihm entfernt verwandte, wohlhabende Person oder auch ein Unbekannter sich in einer temporären finanziellen Zwangslage befindet. Durch Identitätsverschleierung geht die Integrität der E-Mails verloren.

Der Empfänger wird dann beispielsweise um die Möglichkeit gebeten, Gelder auf seinem Konto zu deponieren, um sie vor dem Zugriff der „Nigerianischen Regierung“ zu „retten“. Zuvor soll er allerdings seine Kontendaten angeben (um so unberechtigten Zugriff auf das Konto zu ermöglichen) oder, und dies ist der übliche Weg, einen vergleichsweise „geringen“ Vorschuss an den Sender zahlen.

Die Texte sind in zahllosen Variationen im Internet vorhanden. Nach Schätzungen der nigerianischen Polizei gibt es wöchentlich ca. 30.000 unseriöse Geschäftsofferten per

32 Es handelt sich, wie bei manchen anderen Beispielen auch, um einen seit etwa 20 Jahren aus der Briefpost bekannten Trick, der durch die kostengünstige elektronische Verbreitung zu einem weltweiten Massenphänomen geworden ist.

Brief, Fax oder elektronischer Post aus Nigeria. Es wird angenommen, dass ca. ein Prozent der Offerten zu direkten Kontakten führen und dann Schäden in Millionenhöhe verursachen.[33]

Es handelt sich in der Regel um „Vorkasse-Betrug". Folgende Grundzüge sind darin üblicherweise zu finden:[34]

- Eine hohe Geldsumme wird an den Absender aus einem Vertrag mit der Nigerianischen Regierung ausgezahlt,
- der Absender behauptet, ein Regierungsbeamter oder für die Regierung tätig zu sein,
- der Absender ist gewillt, einen Anteil seines Gewinns (üblicherweise zweistellige Millionenbeträge in US-Dollar) an den Empfänger zu überweisen, wenn dieser sein Konto für den Geldtransfer zur Verfügung stellt,
- Geheimhaltung wird gefordert, um die Aktion vor korrupten Regierungsbeamten zu schützen,
- sehr häufig werden Organisationen wie die Central Bank of Nigeria (CBN) oder die Nigerian National Petroleum Company (NNPC) ohne ihr Wissen in der E-Mail genannt, um Seriosität zu suggerieren.

Das Internet Fraud Complaint Center (IFCC), eine Kooperation zwischen der US-amerikanischen Bundespolizei Federal Bureau of Investigation (FBI) und des National White Collar Crime Center (NW3C), beziffert die durchschnittlichen Schäden durch die sog. „Nigeria Connection" für das Jahr 2004 bei den bekannt gewordenen Fällen auf 3.000 US-Dollar pro gemeldetem Fall. Damit verursacht dieser Trick die zweithöchsten Schäden nach Scheckbetrug über das Internet (3.600 US-Dollar im Durchschnitt).[35] Allerdings machen diese Betrügereien nur 0,2 Prozent aller Beschwerden an das IFCC aus: 415 Personen meldeten einen Betrug, von diesen berichteten 52% über finanzielle Schäden. Es ist davon auszugehen, dass ein Großteil der Fälle im Dunkelfeld bleibt, da die Betroffenen häufig auf eine Anzeige verzichten, um sich Peinlichkeiten zu ersparen.

Auch in Deutschland führen diese E-Mails zu relevanten Schäden. Für das Jahr 2001 wurde in Deutschland bundesweit ein Schaden von 1,63 Millionen Euro durch „Nigeria-Offerten" registriert.[36]

---

33 Polizeiliche Kriminalprävention der Länder und des Bundes (2003): Infoblatt, Thema: Vorauszahlungsbetrug „Nigeria-Briefe".

34 Eine Auflistung findet sich bei der Metropolitan Police London (http://www.met.police.uk/fraudalert/419how.htm).

35 IC3 2004 Internet Fraud - Crime Report January 1, 2004—December 31, 2004, S. 3.

36 Polizeiliche Kriminalprävention der Länder und des Bundes (2003): Infoblatt, Thema: Vorauszahlungsbetrug „Nigeria-Briefe",

5.2.4 Verbreitung von Malware

In vielen Fällen wird die Versendung von Spam dazu genutzt, Malware, also schädigende Softwareprogramme, massenhaft zu verbreiten. Diese Form von Spam bedroht vor allem die Verfügbarkeit von Daten auf dem heimischen Rechner oder am Arbeitsplatz. Das Ziel der Angreifer ist in manchen Fällen die Verbreitung eines schädigenden Programms. Der „Erfolg“ bemisst sich nach der Schadenswirkung und der Resonanz in den Medien auf die Viren oder Würmer.

Darüber hinaus wird Malware auch verbreitet, um einen Rechner mit einer Hintertür zu versehen. Sogenannte Trojaner sorgen dafür, dass Dritten Zugriff auf den befallenen Computer über das Internet ermöglicht wird, etwa um auf Kosten dieses Nutzers zu Surfen oder diesen PC als Basis für die Verbreitung von Spam zu verwenden. Dieses Vorgehen fällt in Deutschland unter den Straftatbestand der Computerkriminalität. Das Ausspähen von Daten durch Unbefugte, die gegen unberechtigten Zugang besonders gesichert sind, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft (StGB § 202a Ausspähen von Daten).

Welche Schäden durch Trojaner oder andere Viren jährlich verursacht werden, ist zwar nicht zuverlässig zu bestimmen, Schätzungen, wonach sich diese Schäden auf Milliardenbeträge summieren, scheinen jedoch plausibel. Ein in Deutschland öffentlich gemachter und von polizeilicher Seite sehr detailliert untersuchter Fall des Internet-Account Missbrauchs durch Trojaner und anderes Ausspähen von Zugangsdaten nennt eine Schadenshöhe von 4,5 Mio. Euro. Der Fall betrifft die Schäden der Kunden bei einem einzigen Internet-Provider im Jahr 1999.[37]

5.3 Anforderungen und zentrale Probleme der Bekämpfung

5.3.1 Identitätsverschleierung

5.3.1.1 Gefälschte Header

Die einzelnen Elemente des Headers einer E-Mail sind alle fälschbar. Die Angaben lassen sich per Hand eintragen. Ein Spammer kann so den Weg einer E-Mail über vertrauenswürdige Mail-Agenten vortäuschen, indem er falsche Eingaben in den Header macht und so die Integrität des Headers verfälscht.

---

37 Vick/Roters (2003), S. 9. Die Studie diente u.a. dazu, Erkenntnisse über die Sozial- und Persönlichkeitsstruktur der Täter zu gewinnen.

Erst wenn die E-Mail in den Bereich des Empfängers gerät und vom eigenen Mail Delivery Agent angenommen wurde, ist die Absender-Adresse durch den Empfänger zuverlässig bestimmbar. Kennt man mehrere der in den Transfer eingebundenen Mail Transfer Agents, weil es sich um das eigene System oder das des Providers handelt, ist von einer vertrauenswürdigen Quelle auszugehen.

Abbildung 5-5: Gefälschte Elemente eines E-Mail-Headers

Microsoft Mail Internet Headers Version 2.0

Received: from **gigdig.com** ([218.145.253.162]) by xxxxx.WIKGMBH.ORG with Microsoft SMTPSVC(5.0.2195.6713);
Tue, 7 Jun 2005 04:16:06 +0200
Received: **from choiceoffers.73674737.lightsped.net (iris2.directnic.com** [204.251.10.82])
by gigdig.com with esmtp
id 518E657483 for <xxxxx.xxxxx@wik.org>; **Mon, 06 Jun 2005 19:15:56 -0700**
Message-ID: **110001c56b06$695c9e3c$e622fef6@choiceoffers.73674737.lightsped.net**
From: **"Childishness H. Disaster" unbuckle@choiceoffers.73674737.lightsped.net**
To: A xxxxxx.xxxxxx@wik.org
Subject: How about your good xxx?
Date: Mon, 06 Jun 2005 19:15:56 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="----=_NextPart_000_0025_E65E4449.F6CC158E"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2800.1437
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1081
X-Virus-Scanned: Norton
Return-Path: unbuckle@choiceoffers.73674737.lightsped.net
X-OriginalArrivalTime: 07 Jun 2005 02:16:07.0846 (UTC) FILETIME=[DD67A460:01C56B06]
------=_NextPart_000_0025_E65E4449.F6CC158E
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
------=_NextPart_000_0025_E65E4449.F6CC158E
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable
------=_NextPart_000_0025_E65E4449.F6CC158E--

---

wik CONSULT

Quelle: WIK Analyse (vermutlich gefälschte Elemente sind fett gedruckt)

Das einzige nicht ohne größeren Aufwand fälschbare Element ist die IP-Adresse des sendenden Mail Transfer Agents.[38] Dies gilt jedoch nur für die Ziffernfolge, nicht für die damit verbundene Domain.

---

38 Vgl. BSI (2005), S. 67. Zumindest sei der Aufwand so groß, so die Aussage der Studie, dass dies in der Praxis keine Rolle spiele. Jemand, der IP-Adressen fälsche, könne damit „ganz anderen Schaden“ anrichten.

5.3.1.2 Gefälschte WHOIS-Einträge

Rund 318 Mio. Hosts existierten Anfang Juni 2005 im Internet, d.h. in diesem Fall Domain Names, die mit einer IP Adresse verbunden sind.[39] Unter den wichtigsten Top Level Domains (gTLD) .com, .net, .org, .info, .biz sind zurzeit rd. 52 Mio. Domain Names registriert, unter den beliebtesten Länderdomains (ccTLD) .de, .uk, .nl, .it und .us zusammen etwa 16 Mio.[40]

Name und Adresse des Registranten einer Domain lassen sich über das verteilte Datenbanksystem Whois von jedem Internet-Account abfragen. Bei der Registrierung einer Domain werden diese Daten vom Registrar (häufig der Internet Service Provider) abgefragt und eingetragen. Auf eine weitergehende Identifizierung wird zumeist verzichtet. Es muss daher vermutet werden, dass die Anzahl der versehentlich oder absichtlich gefälschten Daten hoch ist und es für Spammer keine Mühe bedeutet, falsche Angaben eintragen zu lassen.

Im vergangenen Jahr 2004 gingen bei der ICANN (Internet Corporation for Assigned Names and Numbers) 31.533 Hinweise auf potentiell falsche Whois-Daten ein. Diese Hinweise wurden von ICANN gesammelt und die Beschwerdeführer um Aufklärung gebeten. Zusätzlich haben ICANN-Mitarbeiter ungeklärte Fälle selbst überprüft.

Erfasst werden die Meldungen im jährlichen "Whois Data Problem Reports System" (WDPRS).[41] Die Zahl der monatlichen Meldungen im System ist (gemittelt) von 1.342 im Vorberichtszeitraum auf 2.865 Meldungen angestiegen. ICANN wertet dies als Beweis, dass das System im Jahr 2004 bekannter geworden ist und daher häufiger verwendet wird. Einen Rückschluss auf die Gesamtzahl der falschen Einträge lässt der Bericht nicht zu. Offenbar stehen aber die meisten Meldungen im Zusammenhang mit Spam-Versand. In 80 Prozent der Fälle wurde Spam als der Grund für die Beschwerde angegeben. Die ICANN-Experten schätzen anhand ihrer Auswertung zwei Drittel der Fälle als aufklärbar ein. Bei 10 Prozent handele es sich um echte Verstöße gegen die Whois-Policy.

Prinzipiell könnten Spammer somit anhand ihrer Domains identifiziert werden. Das dazu verfügbare Datenbanksystem weist jedoch strukturelle Probleme auf. Die Eintragungen werden kaum kontrolliert. Angesichts der weltweiten Verbreitung der WWW-Nutzung und der hohen Anzahl der Domains erscheint eine eingehende Prüfung jedes Registranten undurchführbar, und zwar nicht zuletzt deshalb, weil eine solche zuverlässige Kontrolle internationale Vereinbarungen über die anzuwendenden Authentifizierungsverfahren voraussetzen würde.

---

39 Siehe www.isc.org. Die Statistik erfasst die Anzahl der IP Adressen, die einem Domain Name zugeordnet sind.
40 Vgl. dazu die Statistiken des deutschen Network Information Centers unter www.denic.de.
41 ICANN 2005.

5.3.1.3 Zombie-PCs und Botnetze

Als Zombie-PC bezeichnet man einen Computer mit Internet-Zugang, der durch Würmer, Viren, Trojaner, direkte Angriffe oder ähnliches vom Nutzer unbemerkt unter die Kontrolle eines Spammers gebracht worden ist. Die Systeme werden dann dazu genutzt, um unerkannt Spam zu verbreiten bzw. auch um weitere Zombie-PCs zu besetzen. Da es sich zumeist um große vernetzte Systeme handelt, spricht man auch von „Zombie-Farmen“ oder „Botnetzen“.

Angeblich ist das Vermieten von Botnetzen bereits ein Dienstleistungsgeschäft für Hacker, die diese den Spammern anbieten. Die Zahl der aktiven Zombie-Systeme wird von Experten auf einige Million geschätzt. SW-Produzenten von Anti-Malware beobachten die Entwicklung von Zombie-Systemen sehr genau. Beispielsweise betreibt Symantec, einer der Marktführer für Security-Software, Forschung auf diesem Gebiet.

Mehr als eine Mio. Computer sind weltweit zu so genannten Zombie-PCs mutiert, die von Angreifern übernommen wurden und von denen Spam und Viren verbreitet werden. Dies geht aus einer Erhebung der internationalen Nonprofit-Forschungsvereinigung Honeynet Project (http://www.honeynet.org) hervor. Das Honeynet Project hat für seine Untersuchung mehr als 100 Botnets überwacht. Das größte derartige Netzwerk bestand aus 50.000 infizierten PCs.[42]

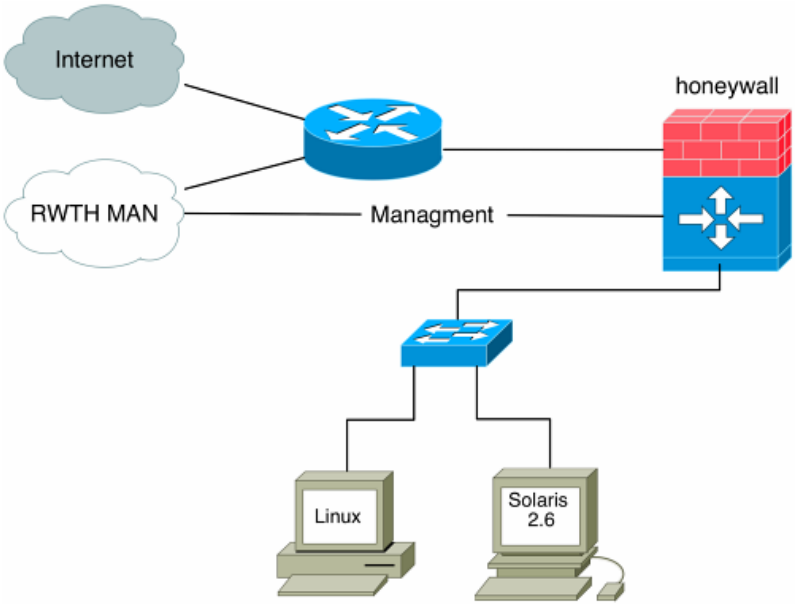
In Deutschland ist ein Kooperationspartner des weltweiten Projekts an der RWTH Aachen, Laboratory for Dependable Distributed Systems, angesiedelt. Die Forscher betreiben seit Januar 2004 ein Honeynet und haben erste Ergebnisse veröffentlicht.[43]

Ziel des Projekts ist, das Verhalten von Botnet-Betreibern zu beobachten und die Funktionsweise von Botnets zu verstehen, um Gegenmaßnahmen ergreifen zu können. Dazu wurde ein Honeynet-System mit dem Internet verbunden. Die Honeywall spiegelt möglichen Angreifern ein funktionierendes System mit Inhalten vor (z. B. E-Mails, Excel-Spreadsheets oder verschlüsselte Daten). Spezielle Software beobachtet den eingehenden Traffic und blockiert ausgehende Angriffe.

---

42 Honeynet Project and Research Alliance (2005a).
43 http://www-i4.informatik.rwth-aachen.de/lufg/research/projects/honeynet/honeynetproject.en.html, Honeynet Project & Research Alliance (2005b).

Abbildung 5-6: Schematischer Aufbau des Honeynet-Projekts Deutschland



Quelle: Lehr- und Forschungsgebiet Informatik 4, Verlässlichkeit in verteilten Systemen, RWTH Aachen

Die bisher vorliegenden Ergebnisse des Projekts lassen den Schluss zu, dass sogar passive Systeme ohne ausgehenden Traffic im Internet Angriffe provozieren. Der erste Angriff erfolgte zehn Minuten nach Anschluss des Honeypot an das Internet (Port Scans). Nach Ausweitung des Versuchs mit einem größeren Honeypot-Netz konnten Angriffsversuche von 48.000 verschiedenen IP-Adressen identifiziert werden. Würmer und andere Malware wurden häufig beobachtet. Mehr als 90 Prozent aller Angriffe gingen von Windows Systemen aus. In der Regel handelt es sich nach den Vermutungen der Forscher um DSL-Verbindungen.

Botnets machen laut Eco-Verband einen Großteil des Spam aus.[44] Manche Schätzungen gehen von bis zu 70 Prozent aus. Es scheint aufgrund der bisherigen Forschungsergebnisse plausibel, dass Botnets von qualifizierten und spezialisierten Angreifern betrieben werden. Vermutlich handelt es sich heute kaum noch um Einzeltäter, sondern um Gruppen mit kriminellen Strukturen. Das künftige Schadenspotenzial dieser organisierten Aktivitäten kann daher nicht hoch genug eingeschätzt werden.

44 Eco White-Paper, S. 7.

5.3.2 Absichtsverschleierung

Dass Spam-Nachrichten den Empfänger über die Absichten des Senders sowohl in der Betreffzeile als auch im Nachrichtentext möglichst im Unklaren lassen, gehört zu den Selbstverständlichkeiten. Die Betreffzeile suggeriert z. B., dass dem Empfänger der Absender bekannt ist („Remember me?“, „How are you?“, „You don´t know me from Adam.“)

Immer wichtiger wird es außerdem für die Spammer, die Ausfilterung von Spam-Mails anhand von Wortverdrehungen und der Benutzung von Sonderzeichen zu erschweren. Dazu werden Methoden der „Leetspeak“[45] verwendet oder auch sog. UCE-Begriffe kreiert, z. B. vi4gr4 oder \/|ágrà, h4110 (hallo) oder auch |-|4|_|_0.

Weitere Beispiele sind das Auslassen von Leerzeichen („Buydrugsonline“) oder das Einfügen von Leerzeichen oder Sonderzeichen („M O R T G A G E“, „ F*R*E*E V’I’A’G’R’A O*N*L*I*N*E”).

Des Weiteren existieren zahlreiche Möglichkeiten, Spam-Filter mit verschiedenen Tricks auszuschalten, z. B. durch Ausnutzung von Schwächen von Microsoft Internet Explorer, HTML und verschiedenen Möglichkeiten, Tags einzufügen.[46]

5.3.3 Aussendung aus dem Ausland

Spam wird in der Regel nicht aus Deutschland, sondern aus dem Ausland versandt. Hauptsächlich erhalten Nutzer Spam in englischer Sprache. Dies hat scheinbar den Vorteil für die Spammer, weltweit verständlich zu sein, bzw. vor allem diejenigen Nutzer zu erreichen, die im herausragenden Herkunftsland des Spam wohnen (der Hauptteil des Spam stammt aus den USA).

Besonders zahlreich sind die unerwünschten Massenaussendungen aus Ländern mit unzureichender Datenschutzgesetzgebung wie z. B. den USA und aus Ländern, in denen IT-Sicherheitsstandards weniger hoch sind, so dass Rechner mittels Malware als ferngesteuerte Mailserver von Spammern genutzt werden können. Dies gilt vermutlich für Spam aus Südkorea.

Statistiken über die Herkunft von Spam weltweit können nicht auf repräsentativen Erhebungen beruhen, da sich aus allen vorhandenen Spam-Mails keine echte Zufallsstich-

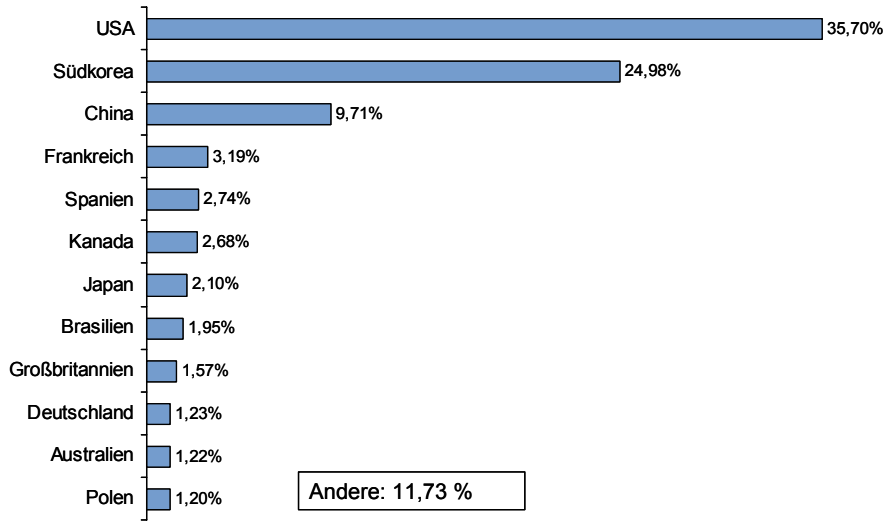
---

45 Der Begriff stammt aus der Welt der jugendlichen Computernutzer. „Leet“ bedeutet soviel wie „Elite“ (engl.) was soviel wie „Computernutzer-Elite“ heißen soll. Der Begriff lässt sich auch mit den Ziffern 1337 (auf dem Kopf stehend zu lesen) ausdrücken. Dieses Beispiel verdeutlicht bereits das Prinzip der Erschaffung von Leetspeak-Begriffen: Lautmalerische Ausdrücke kombiniert mit Ziffern und Zeichen (vgl. dazu die Ausführungen bei Wikipedia).

46 Eine Auflistung findet sich bei dem Spam-Filter Hersteller Sophos, http://www.sophos.com/spaminfo/explained/fieldguide.html.

probe ziehen lässt. Anbieter von Anti-Spam-Tools führen jedoch im eigenen Interesse Untersuchungen durch, die eine Näherung an die Herkunftsländer von Spam erlauben. Der brititsche Softwarehersteller Sophos veröffentlicht regelmäßig eine Liste mit Ländern, aus denen die meisten Spam-Mails stammen. Die Forscher der SophosLabs analysierten dafür alle E-Mails, die in ihren weltweit eingerichteten fiktiven E-Mail-Konten (sog. Honey-Pots) über einen bestimmten Zeitraum eingehen. Danach führen die USA mit weitem Abstand von rund 36% Anteil am weltweiten Spam-Aufkommen die Liste der Versender an (vgl. Abbildung 5-7). Darauf folgt Südkorea mit rd. 25% aller Spam-Mails. In Deutschland stellt der Versand von Spam ein weitaus geringeres Problem dar. Von hier stammen nur 1,23% der unerwünschten Mails.

Abbildung 5-7: Spam-Versender nach Ländern (Schätzung)



Quelle: Sophos GmbH

Aufgrund der regelmäßigen Erhebung kann die Studie feststellen, dass der Anteil der Spam-Mails aus den USA seit Inkrafttreten des CAN-Spam Acts im Jahr 2003 deutlich um über 10% Prozent gesunken ist. Ob hier ein Ursache-Wirkungsverhältnis nachweisbar ist, müssten jedoch weitere Untersuchungen erst noch zeigen.

5.3.4 Post- und Fernmeldegeheimnis

Die Filterung von E-Mails zum Zweck der Spam-Vermeidung stößt dort auf rechtliche Grenzen, wo einerseits das Telekommunikationsgeheimnis und die Persönlichkeitsrechte der Nutzer betroffen sind. Andererseits besteht ein berechtigtes Interesse für

z. B. ein Unternehmen, Datensicherheit zu gewährleisten und Schäden durch Spam zu vermeiden sowie für die Nutzer, die Ressourcenbeanspruchung durch unerwünschte Massenaussendungen einzudämmen.

Das Spannungsfeld der Spam-Filterung ist daher Gegenstand der aktuellen rechtlichen Diskussion und nicht allein ein Problem der technischen Realisierung. Die entsprechenden Bestimmungen über das Fernmeldegeheimnis im Grundgesetz Art. 10 sowie § 206 Abs. 2 Nr. 2 im StGB bilden den Rahmen für die Rechtmäßigkeit der Filterung:

GG Art. 10

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.

(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. [...]

§ 206 Abs. 2 Nr. 2 StGB

„(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder

3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,

2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder

3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.“

Daraus ergibt sich, dass eine Filterung von „allen“ Spam-verdächtigen E-Mails ohne Einverständnis des Nutzers nicht pauschal zulässig sein kann, da es gegen das GG Art. 10 verstößt. Der Tatbestand des „Unterdrückens“ wird durch eine Ausfilterung erfüllt.

Dabei ist es unerheblich, ob es sich um Zurückhalten, Umleiten oder Verstümmeln oder Löschen handelt. Allenfalls kann es gerechtfertigt sein, für das Datenverarbeitungssystem schädliche E-Mails herauszufiltern.[47] Die Löschung von False Positives, also augenscheinlichen Spam-Mails, bei denen es sich aber um „Ham", also gewünschte E-Mails handelt, ist somit für den Betreiber des Spam-Filters äußerst problematisch. Es ist ein anzuerkennendes Problem, dass sich das Risiko der Löschung von False Positives nie ganz ausschließen lässt.

Vor dem Hintergrund des Post- und Fernmeldegeheimnisses bedeutet Spam-Filterung somit, dass

- das Einverständnis des Nutzers eingeholt werden muss, wenn Filter verwendet werden,
- die Entscheidung über den Umgang mit dem ggf. zentral technisch gekennzeichneten Spam dem Nutzer überlassen bleibt (nutzerbezogene Lösung).

Die Spam-Filterung wird nicht von der Problematik des Post- und Fernmeldegeheimnis berührt, wenn

- in einem Unternehmen keine TK-Dienste für Nutzer erbracht werden (d. h. z. B. wenn in einem Unternehmen die private E-Mail-Nutzung nicht gestattet ist),
- es sich um Schutzmaßnahmen zur Sicherstellung der Datenverarbeitung handelt (allerdings sollten die Nutzer aus Verhältnismäßigkeitsgründen von der Filterung in Kenntnis gesetzt bzw. eine Quarantäne-Lösung bevorzugt werden).

ISP wie T-Online oder AOL sehen sich aufgrund der Bestimmungen mit Rechtsunsicherheiten konfrontiert. Einerseits wollen sie ihren Kunden Anti-Spam-Dienstleistungen anbieten, andererseits könnten sie damit gegen das Post- und Fernmeldegeheimnis und gegen die Transportpflicht der Provider nach TKG verstoßen. Besonders kundenunfreundlich ist die Einlieferung von Spam in das elektronische Postfach, wenn es sich um Malware handelt. Eine Lösung könnte sein, die Unternehmen unter bestimmten Voraussetzungen von dieser Pflicht zu entbinden. Zum Beispiel könnten schädliche E-Mails geblockt werden, wenn der Nutzer davon in Kenntnis gesetzt wird.

---

47 Köcher (2005), S. 165. Der Autor beschäftigt sich mit der bisher einzigen obergerichtlichen Entscheidung zur Frage einer möglichen Strafbarkeit der Ausfilterung von E-Mails durch Mitarbeiter eines Unternehmens, welche grundsätzliche Bedeutung für die Frage der Grenzen einer Filterung besitzt (OLG Karlsruhe, Beschluss v. 10. Januar 2005, Az.: 1 Ws 152/04).

5.4 Folgen: Kosten durch Schäden und künftige Schadensentwicklung

Die gesamte Kostenbelastung für ISP sowie private und geschäftliche Nutzer durch Spam ist nur schwer exakt zu bestimmen. Zahlenmaterial liegt dazu zwar vor, es handelt sich aber zumeist um Schätzungen von Messaging-System-Anbietern, die Berechnungen für die Kosten von Spam ohne bzw. mit Anti-Spam-Lösungen vorliegen. Ziel ist häufig aufzuzeigen, dass sich die Implementierung dieser Lösungen für ein Unternehmen lohnt.

Beispielsweise ist es problematisch, die aufgewendete Arbeitszeit für die Bekämpfung von Spam zu benennen. Dieser Bereich macht vermutlich einen erheblichen Teil der Kosten aus. Zum Einen wendet jeder E-Mail-User pro Tag einige Minuten für das Löschen von Spam auf, zum Anderen wächst auch der Zeitaufwand für die IT-Abteilungen in Unternehmen. Eine Befragung des Marktforschungsunternehmens IDC von 2004 bei 1.000 IT-Managern kommt etwa zu dem Ergebnis, dass das IT-Personal ohne Anti-Spam-Maßnahmen 43 Minuten, mit Maßnahmen 19 Minuten täglich aufbringen muss. Ein Nutzer benötigt für das Löschen seiner Spam-Mails 10 bzw. 5 Minuten. Je nach Größe eines Unternehmens und je nach Stundenlohn entstehen somit durch Spam spezifische Kosten, die die Produktivität eines Unternehmens beeinträchtigen.[48]

Die Kosten für Spam lassen sich auch deshalb mittels empirischer Untersuchungen kaum bestimmen, da die Mehrzahl der Unternehmen nicht in der Lage ist, die Total Cost of Ownership (TCO) ihrer Message-Management-Infrastruktur zu beziffern. Nach einer Untersuchung des britischen Unternehmens BT-Security vom Herbst 2004[49] schätzen die Unternehmen des Finanzdienstleistungssektors die Bedrohung durch Spam als steigend ein und erwarten künftig höhere Kosten für die Bekämpfung. Erwartet wird, dass sich die Kosten durch Outsourcing des Message-Managements reduzieren lassen.

Eine ausführliche Schätzung der Kosten von Spam und Anti-Spam-Maßnahmen hat das BSI im Jahr 2005 vorgelegt.[50] In der Studie werden unmittelbare Kosten für Traffic, die Nutzung von Mailserver- und Storage sowie das zusätzliche IT-Personal benannt, mittelbare Kosten durch Produktivitätsverlust bei den Mailempfängern (Zeitaufwand), Kosten durch eingeschränkte Erreichbarkeit und Verfügbarkeit sowie für die Reparatur beschädigter oder überlasteter Systeme und schließlich sonstige Kosten. Diese bestehen aus Verlusten durch Imageschäden, z. B. wegen des unwissentlich eigenen Versands von Spam (etwa durch Zombie-PCs) und die Kosten für Werbung und Marketing, um den Imageschaden wieder auszugleichen bzw., bei ISP, um für die eigenen Anti-Spam-Lösungen zu werben.

---

48 ZDNet vom 21. April 2004, „Spam kostet täglich bis zu 43 Minuten Arbeitszeit."
49 www.antispamday.de/facts.html
50 Vgl. BSI (2005), S. 30ff.

In der Berechnung wird von einer durchschnittlichen Größe einer Spam-Mail von 25 KByte ausgegangen. Es wird außerdem angenommen, dass jeder Account 5 Spam-Mails pro Tag erhält (vgl. Tabelle 4-1).

Tabelle 5-3: Kosten von Anti-Spam-Maßnahmen für verschiedene Unternehmenstypen (Schätzung)

	großer ISP	mittlerer ISP	Großunternehmen	KMU	Kleinunternehmen
Aktive Postfächer	3 Mio.	50.000	5.000	500	5
Spam-Mails pro Tag	15 Mio.	250.000	25.000	2.500	25
IT-Umgebung	-	-	eigene IT-Abteilung	keine IT-Abteilung	keine IT-erfahrenen Mitarbeiter
Unmittelbare Kosten p.a.	1 Mio.	120.000	150.000	35.000	25
Mittelbare Kosten p.a.	60.000	-	85.000	15.000	-
Sonstige Kosten p.a.	150.000	10.000	-	-	-
Kosten durch Spam p.a. (mit Anti-Spam-Maßnahmen)	225.000	60.000	85.000	9.000	300
Kosten durch Spam p.a. (ohne Anti-Spam-Maßnahmen)	1,43 Mio.	190.000	320.000	59.000	325
Kosten pro Spam-Mail (mit Anti-Spam-Maßnahmen)	0,026 Cent	0,2 Cent	4 Cent	6 Cent	4 Cent
Kosten pro Spam-Mail (ohne Anti-Spam-Maßnahmen)	-	-	18 Cent	18 Cent	66 Cent
Kosten in Euro					

Quelle: BSI 2005

Es zeigt sich, dass sich für die Unternehmen die Anzahl der Spam-Mails und die damit verbundenen Kosten erheblich reduzieren lassen. Dies gilt vor allem für große und mittlere ISP sowie für Großunternehmen und KMU. Die Kosten pro Spam-Mail lassen sich mit geeigneten Lösungen vor allem bei Kleinunternehmen stark senken. Durch das geringe Spam-Aufkommen ist jedoch die gesamte Ersparnis durch den Einsatz von Anti-Spam-Maßnahmen als eher klein einzuschätzen. Der Anreiz für Unternehmen dieser Größe, entsprechende Lösungen zu implementieren erscheint daher kaum vorhanden. Dies ist insofern problematisch, als Kleinunternehmen mit 1,3 Mio. die zahlreichste Un-

ternehmensgrößenklasse bilden. Die volkswirtschaftliche Belastung durch (ungefilterten) Spam ist also erheblich einzuschätzen. In diesem Beispiel beläuft sich die Summe auf rd. 422,5 Mio. Euro pro Jahr. Außerdem besteht das Risiko, dass diese Unternehmen ohne entsprechende Schutzmaßnahmen zum bevorzugten Ziel der Spammer werden.

6 Bedrohung durch neue Formen der unerwünschten Massenaussendungen am Beispiel von Spit

Das Jahr 2004 gilt unter Experten als das Jahr „Null“ für die Verbreitung von Voice over IP (VoIP) im Massenmarkt. Während VoIP sich in der Unternehmenskommunikation sowohl bei den Telekommunikationsanbietern (insbesondere im Backbone) als auch in der gewerblichen Wirtschaft schon seit einigen Jahren in Anwendung befindet, mussten für die massenhafte Anwendung in öffentlichen Netzen in den letzten Jahren erst zahlreiche technologische Verbesserungen (neue Protokolle, Softswitches) realisiert und implementiert werden, um privaten Haushalten bei VoIP die gleiche Qualität wie bei der leitungsvermittelten Sprachkommunikation anbieten zu können. Mittlerweile benutzen in Deutschland rund 500.000 Kunden diese Technologie und es ist im Prinzip eine Frage der Zeit, wann das Public Switched Telephone Network (PSTN) komplett auf paketvermittelnde Übertragung umgestellt wird.

Mit der Migration des PSTN zu einer „all IP“ basierten Netzinfrastruktur sind eine Reihe von technischen Änderungen in der Systemarchitektur verbunden, die VoIP anfällig machen für die sprachbasierte Übermittlung von unerwünschten Massenaussendungen. Damit IP-basierte Sprachtelefonie in öffentlichen Netzen funktioniert, wurden verschiedene standardisierte Protokolle implementiert. Es zeichnet sich ab, dass sich das von der Internet Engineering Task Force (IETF) ins Leben gerufene Session Initiation Protocol (SIP) gegenüber dem konkurrierenden ITU Standard H.323 künftig durchsetzen wird. SIP stellt ein Kontrollverfahren der Anwendungsschicht zum Aufbau, zur Ablaufsteuerung und zum Beenden von Multimedia-Sessions mit zwei oder mehr Teilnehmern dar, das dementsprechend auch für die Vermittlung von VoIP geeignet ist. Um ein Gespräch über VoIP mit einem Dritten führen zu können, muss zunächst dessen IP-Adresse gefunden werden. Dann wird unter Angabe der eigenen IP-Adresse der Verbindungswunsch signalisiert und die Parameter des Austauschs werden ausgehandelt bzw. festgelegt.

Typischerweise erfolgt ein Rufaufbau über einen Proxy-Datenserver, der als Vermittlungsstelle agiert und die Authentikation, die Autorisierung, die Netzzugangskontrolle sowie das Routing der Datenpakete übernimmt. Abgesehen von den auf der IP-Ebene „übernommenen“ traditionellen Bedrohungen (z. B. Mitlesen von Paketen) bestehen bei SIP/VoIP spezifische Angriffs- bzw. Missbrauchsmöglichkeiten in der Anwendungsschicht.[51] Experten gehen davon aus, dass sich durch die Migration zur IP-basierten Sprachtelefonie die Sicherheitslage mit Blick auf die Verfügbarkeit, Vertraulichkeit und die Integrität allgemein deutlich verschlechtern wird.[52] Zu den derzeit in der Öffentlichkeit am häufigsten diskutierten Missbrauchsformen gehört insbesondere Spamming over IP-Telefonie (Spit). Daneben werden die Beeinträchtigung von Anrufbeantworter-

---

51 Vgl. Graydon (2005), S. 55ff.

52 Vgl. z. B. Lutz (2005), S. 58ff. Vom Einsatz von VoIP in sicherheitsrelevanten Bereichen raten Experten daher derzeit ab.

funktionen sowie Spoofing und Denial of Service-Attacken etwa durch Malformed Messages diskutiert.[53]

- Spit

Spit stellt für unseriöse werbetreibende Unternehmen ein attraktives Medium der Direktvermarktung dar, das durch Automatisierung wesentlich kostengünstiger realisiert werden kann als etwa durch Call Center. Durch die Kostenvorteile bei VoIP in Verbindung mit dem Einsatz von Sprachservern lassen sich im Minutentakt Tausende von Anrufen („Invite-Anrufe“) tätigen. Die Nummernlisten können hierbei flächendeckend durch Zufallsgeneratoren selbst erzeugt werden. Dieses Geschäftsmodell basiert in der Regel auf der Initiierung eines Rückrufes über kostenträchtige Nummern für Mehrwertdienste (0190- oder 0900-Nummern). In manchen Fällen wird der Kunde aufgefordert, einen Rückruf über das Drücken einer entsprechenden Tastenkombination zu initialisieren, ohne dass für ihn unmittelbar ersichtlich ist, dass das Gespräch über eine kostenträchtige Mehrwertdienstenummer geführt wird und auch kein Hinweis auf die dadurch entstehenden Kosten erfolgt.

Unabhängig von diesen in der Regel erst durch die Telefonabrechnung erkennbaren Missbrauchsformen kann jedoch alleine schon der (wiederholte) Spit-Anruf zu einer störenden Belästigung der normalen Telefonfunktionalität führen.[54] Dies gilt insbesondere dann, wenn im Ausland dislozierte Anruf-Computer zeitversetzt ihre Anrufe z. B. am Tag aus den USA nach Europa tätigen. Es kann vermutet werden, dass die Belästigung schon durch wenige Spit-Anrufe von den Endkunden als wesentlich intensiver und nachhaltiger empfunden wird als bei Spam, da hierbei durch Asynchronität der Kommunikation ein gewisser Schutzmechanismus besteht.

- Beeinträchtigung von Anrufbeantworterfunktionen

Ein weiteres Problem durch Spit entsteht durch die in der Regel als WAV-Datei versendeten Werbebotschaften. Eine 30-sekündige Sprachnachricht erreicht ein halbes Megabyte und kann insbesondere bei gehäuften Versendungen (Voicemail-Bombing) schnell zu einer vollständigen Speicherbelegung eines Anrufbeantworters oder einer Voicemailbox führen. Dies dürfte, insbesondere bei Mobilfunknutzern, schon bei wenigen Voicemails zu einer deutlich erschwerten Handhabung oder zu einem Ausfall der Anrufbeantworterfunktion führen.

---

53 Vgl. Graydon ebenda, S. 56f. Weitere Angriffsmöglichkeiten bestehen z. B. bei schwacher Authentifikation in der .de-Registrierung von Kunden in Anbieterverzeichnissen oder auch darin, dass durch das Versenden von Cancel-Befehlen Gespräche unterbrochen oder ganz unterbunden werden können.

54 Vgl. Brodersen (2004).

- Spoofing

Ähnlich wie bei den Phishing-Angriffen bei E-Mail können bei SIP falsche Absenderidentitäten vorgetäuscht werden, die den Angerufenen dazu verleiten können, bestimmte Informationen am Telefon preiszugeben.

- Malformed Messages

Denial-of-Service-Attacken gehören heute zu den maßgeblichen Bedrohungen der Internet-Verfügbarkeit, die z. B. durch die massenhafte Versendung von E-Mails an bestimmte Netzknoten oder Server ausgelöst werden können. Auch bei VoIP sind heute entsprechende Angriffsszenarien nicht auszuschließen. Missgebildete Messages (z. B. falsche Schreibweise des Headers) können von Angreifern aufgrund von Systemintoleranzen dazu genutzt werden, dass SIP-basierte Telefonanlagen (Speicherfehler, Buffer-Overflows) den Dienst einstellen und bestimmte Teilnehmer dadurch für Dritte unerreichbar werden.

Ein zentraler Aspekt, in dem sich Spam und Spit unterscheiden, besteht darin, dass der Versender von Spit auf Grund des SIP-Protokolls sehr viel leichter lokalisierbar ist als der Versender von Spam. Realisiert wird dies durch die genaue Zuordnung der VoIP-Nummern in den einzelnen Anbieter-Netzen sowie über VoIP-Peering wie etwa über ENUM oder Zentralen wie e164.info. Jeder abgehende Anruf signalisiert dem angerufenen Anschluss im Rahmen von SIP die eigene Rufnummer bzw. IP-Adresse. Generell müssen an e164.info angeschlossene Carrier Regeln für die Kooperation akzeptieren und sicherstellen, dass keine anonymen Nutzer-Accounts zugelassen werden. Sollte einer dieser Teilnehmer kostenlose Anrufe („on net-calls“) zu Spit-Zwecken missbrauchen, so kann seine Rufnummer identifiziert und diese von seinem Carrier gesperrt werden. Insofern müssen missbräuchliche Werbeanrufe über VoIP deutlich größere Hürden überwinden als entsprechende Massenaussendungen über E-Mail.

Ein anderer, eher technischer Ansatz, besteht darin, Spit bereits im Backbone zu erkennen und z. B. auf Grund auffälliger Häufungen von Netzkontakten aus bestimmten VoIP-Netzen abzublocken bzw. auszufiltern. Einzelne Anbieter in Deutschland wie z. B. Toplink verwenden ein solches Schutzsystem bereits. Ein Problem bei der Implementierung von Filtersystemen kann darin bestehen, dass diese u. U. zu „scharf“ eingestellt sein können und daher z. T. berechtigte VoIP-Telefonate abblocken.

Derzeit gehen Experten davon aus, dass in Deutschland die Spit-Problematik de facto noch keine Rolle spielt. Dies hängt damit zusammen, dass die Zahl der VoIP-Teilnehmer noch vergleichsweise gering ist und die Migration von IP im PSTN nur schrittweise erfolgt. Allerdings wird in der Presse bereits vereinzelt über entsprechende Vorkommnisse berichtet. Eine der Missbrauchsstrategien scheint darin zu bestehen, dass ein Anrufserver die Responsivität der angerufenen Anschlüsse „testet“. Nimmt ein Teilnehmer den Anruf entgegen, so bestätigt er damit seine Anwesenheit. Der Anrufserver benachrichtigt daraufhin das Personal eines Call Centers über den „positiven“

Kontakt, das dann in einem persönlichen Gespräch mit dem entsprechenden Teilnehmer versucht, ein Produkt oder eine Dienstleistung zu vertreiben.

Trotz der höheren Missbrauchshürden arbeiten VoIP-Anbieter und Software-Hersteller daher intensiv an Mechanismen, um die Sicherheitslage bei VoIP insgesamt zu erhöhen. Zu diesem Zweck wurde im Februar 2005 die Voice-over-IP-Security Alliance (VOIPSA) gegründet, die inzwischen fast 60 Mitglieder zählt und zu der Firmen wie z. B. 3Com, Alcatel, Avaya, MCI, Siemens, Sprint, PriceWaterhouseCoopers, Verisign, AT&T, Symantec oder das SANS-Institut gehören. Eine der wesentlichen Aufgabenstellungen von VOIPSA besteht in der Erforschung der möglichen Risikopotenziale von VoIP und der Untersuchung von Bedrohungsszenarien.

7 Interventionsstrategien und Vorsorge

Ziel von Interventionsstrategien und Vorsorgemaßnahmen ist es, unerwünschte Werbung über elektronische Kommunikationsdienste und den Rufnummernmissbrauch umfassend zu stoppen, ohne dabei die Verlässlichkeit und Funktionalität der Kommunikationsdienste zu beeinträchtigen oder unverhältnismäßig hohe Kosten zu verursachen.

Vor dem Hintergrund des Dilemmas, dass auf der einen Seite die Absender von Spam-Mails

- mit Hilfe des Internet mit weltweitem Aktionsradius agieren,
- ihre Massenaussendungen zu äußerst geringen Kosten realisieren können,
- bereits bei sehr geringer Reaktionsquote hohe wirtschaftliche Anreize besitzen,
- ihre Identität mit relativ einfachen Mitteln verschleiern können,
- permanente Anstrengungen unternehmen, Abwehrmaßnahmen zu umgehen und
- hierbei äußerst flexibel und hochinnovativ vorgehen und sich einer schnell wandelnden Technologie bedienen,

während auf der anderen Seite die Interventionsstrategien zahlreiche Nebenbedingungen erfüllen müssen, wie

- die Funktionalität und Verlässlichkeit der Dienste nicht wesentlich einzuschränken,
- die Kosten für deren Nutzung nicht zu erhöhen,
- die Belange der seriösen Werbewirtschaft und der Wachstumsbranchen E-Commerce und Mehrwertdienste zu berücksichtigen,

wird klar, dass dieses Ziel nicht durch einfache Mittel, sondern nur durch die Kombination verschiedener komplementärer Instrumente auf mehreren Ebenen und durch unterschiedliche Akteure erreicht wird (vgl. Abbildung 7-1).

Als fundamental für alle weiteren Anstrengungen gegen unerwünschte Nachrichten werden klare Rahmenbedingungen durch Gesetze und regulatorische Maßnahmen auf nationaler Ebene betrachtet. Diese müssen zudem eingebunden sein in internationale Vereinbarungen und Kooperationen, um der globalen Dimension dieses Problems gerecht zu werden.

Eine sinnvolle und notwendige Ergänzung finden staatliche- und überstaatliche Maßnahmen in nationalen und internationalen Selbstregulierungsvereinbarungen der Kommunikationsdiensteanbieter und der Direktvermarkter.

Abbildung 7-1: Aufeinander aufbauende Anti-Spam-Maßnahmen (Maßnahmenpyramide)

Quelle: WIK

Neben gesetzlichen, regulatorischen und selbstregulatorischen Maßnahmen, die ein Großteil des Spamming und Rufnummernmissbrauchs direkt beim Verursacher verhindern, spielen technische Maßnahmen zum Abfangen und Ausfiltern unerwünschter Nachrichten eine große Rolle.

Auch langfristig ist davon auszugehen, dass es nicht gelingen wird, auf gesetzlichem Weg und durch Vereinbarungen der Unternehmen Spamming vollständig einzudämmen. Umso bedeutsamer ist es, die Nutzer aufzuklären und zu schulen, damit nicht immer wieder Internet-Neulinge auf bekannte Betrugsversuche hereinfallen bzw. die Mehrzahl der Nutzer über Möglichkeiten der Abwehr von Spam sowie Beschwerdeoptionen informiert ist. Schließlich hat auch das Nutzerverhalten einen entscheidenden Einfluss auf den Einsatz der zur Verfügung stehenden Gegenmaßnahmen und deren Wirksamkeit.

7.1 Internationale Kooperationen

Grundlage des Vorgehens gegen Spam und Rufnummernmissbrauch sind verlässliche Gesetze und regulatorische Rahmenbedingungen zum Schutz der Privatsphäre sowie für die Gewährleistung von Direktmarketingmaßnahmen im Zusammenhang mit elektronischen Kommunikationsdiensten.

Wegen der grenzenlosen Verbreitung der unerwünschten Nachrichten sind nationale Gesetze allein nicht hinreichend, um auf dem Rechtsweg gegen deren Urheber im Ausland vorzugehen. Es bedarf vielmehr einer internationalen Abstimmung. In diesem politischen Prozess besitzen nationale Gesetze gegen Spam noch eine weitere wichtige Funktion. Sie werden als notwendige Verhandlungsgrundlage für internationale Übereinkommen gegen unerwünschte Massensendungen erachtet, da Forderungen auf Basis bestehender nationaler Regelungen eine weit höhere Glaubwürdigkeit besitzen.

7.1.1 Aktivitäten der UN und ITU

Ziele der ITU sind, auf übernationaler Ebene Anti-Spam-Maßnahmen zu koordinieren, und zwar durch die Förderung internationaler Kooperation, die Gestaltung und Vereinheitlichung von Verfahrensgrundsätzen, den Austausch von Informationen und Best practices sowie die Unterstützung von Entwicklungsländern bei der Spam-Bekämpfung.

Beim ersten Teil des von der UN und der ITU organisierten „World Summit on the Information Society (WSIS)“ im Dezember 2003 fand die Spamming-Problematik Eingang in den verabschiedeten Handlungskatalog.[55] Es folgten im Juli 2004 bereits eine WSIS Fachkonferenz[56] zum diesem Thema sowie die Einbeziehung der Spamming-Problematik in die im November 2004 gegründete UN-Arbeitsgruppe zum Thema „Internet Governance“[57]. Weitere Schritte sind nach dem WSIS Gipfel in Tunis zu erwarten.

Die ITU pflegt zudem eine Internetdatenbank zu nationalen Gesetzen gegen Spam, unterstützt die fachliche Auseinandersetzung durch zahlreiche Hintergrundpapiere und fördert den Dialog der Regulierungsbehörden zu diesem Thema beispielsweise im Rahmen des Global Symposium For Regulators im Dezember 2004.[58]

---

55 Vgl. WSIS – Plan of Action, WSIS-03/Geneva/Doc/5-E, Abschnitt C5,d: „Take appropriate action on spam at national and international levels.”
56 Vgl. http://www.itu.int/osg/spu/spam/meeting7-9-04/agenda.html.
57 Vgl. http://www.un.org/news/press/docs/2004/pi1620.doc.htm.
58 http://www.itu.int/osg/spu/spam/index.phtml

7.1.2 Initiativen der OECD

Neben den UN widmet sich auch die Organisation für wirtschaftliche Zusammenarbeit (OECD) der Problematik des enormen Anstiegs von unerwünschten Massensendungen. Seit August 2004 werden die Aktivitäten im Rahmen einer Task Force zu Spam koordiniert. Ziel ist die Unterstützung von Regierungen, nationalen Regulierungsbehörden und der Industrie. Hierfür hat die Task Force ein „Anti-Spam-Toolkit" erarbeitet, das

- ein Regulierungshandbuch umfasst, das als Referenz für die unterschiedlichen Regulierungskonzepte fungieren und weiße Flecken bei der Bekämpfung von Spam aufdecken sowie die internationale Zusammenarbeit bei der Gesetzesdurchsetzung unterstützt,[59]
- eine Untersuchung von Selbstregulierungsvereinbarungen auf Industrie-, nationaler und internationaler Ebene ermöglicht,
- eine Analyse der bestehenden und sich in der Entwicklung befindlichen technischen Maßnahmen gegen Spam erlaubt,
- eine zentrale Datenbank mit Informationen zur Schaffung eines Problembewusstseins gegenüber den Gefahren durch Spam und zur Schulung der Nutzer enthält sowie
- einen Überblick über bestehende Bündnisse gegen Spam, Best Practice Beispiele und Lehren, die aus den ersten Bündnissen gezogen werden können beinhalten soll.[60]

Im Rahmen der Erarbeitung dieses Werkzeugkastens wurden bereits mehrere Workshops und Sitzungen des ICCP-Komitees durchgeführt sowie eine Internetdatenbank zu nationalen Anti-Spam-Gesetzesanwendungen und den jeweils zuständigen Institutionen angelegt. Die Website mit dem Toolkit wird ständig aktualisiert und erweitert.[61]

7.1.3 Vorgaben von europäischer Ebene

Die Europäische Union hat den Handlungsbedarf bei Spam bereits früh erkannt und im Rahmen der E-Commerce-Richtlinie vom 8. Juni 2000 die Problematik von unerwünschten Massenaussendungen thematisiert und Vorgaben zu deren Vermeidung gemacht.[62] So wurde den Mitgliedstaaten aufgetragen, falls sie kommerzielle Massen-

---

59 Das Hintergrundpapier der OECD „Anti-Spam-Regulation" ist am 16.11.2005 erschienen, http://www.oecd.org/dataoecd/29/12/35670414.pdf.

60 Vgl. http://www.oecd.org/document/50/0,2340,en_2649_22555297_33732274_1_1_1_1,00.html.

61 Vgl. http://www.oecd.org/document/24/0,2340,en_2649_22555297_34804568_1_1_1_1,00.html.

62 Vgl. Richtlinie 2000/31/EC des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr"), Artikel 7.

aussendungen gestatten, sie dafür sorgen müssen, dass die Mails in der Betreffzeile als Werbung gekennzeichnet werden und dass Opt-out-Verzeichnisse für natürliche Personen eingeführt werden, an die sich die Diensteanbieter halten müssen.

In Deutschland wurden die Vorgaben dieser E-Commerce-Richtlinie aus dem Jahr 2000 zu Spam nie umgesetzt,[63] dafür aber die weiterreichenden neuen Vorgaben der EU-Datenschutzrichtlinie vom 12. Juli 2002[64], die im Zuge des neuen EU-Rechtsrahmens zur elektronischen Kommunikation gemacht wurden.

Nach Artikel 13 dieser aktuellen Richtlinie müssen die Gesetze in den EU-Mitgliedsstaaten gegen unerwünschte Massenaussendungen vorschreiben,

- dass Teilnehmern, die natürliche Personen sind, nur nach vorheriger Einwilligung (opt-in) von automatischen Anrufmaschinen angerufen werden oder elektronische Werbesendungen (Fax, E-Mail, SMS, MMS etc.) erhalten dürfen.
- Die Regelung enthält die Ausnahme, dass Kunden Werbung für Produkte und Dienstleistungen, die den bereits gekauften ähnlich sind, per elektronischer Post gesendet werden darf, soweit sie dem nicht widersprechen (opt-out).
- Elektronische Werbenachrichten sind auf jeden Fall verboten, wenn die Identität des Absenders verschleiert oder verheimlicht wird oder die gültige Adresse fehlt, an die der Empfänger eine Aufforderung zur Einstellung solcher Nachrichten senden kann.[65]

Welche Maßnahmen geeignet und zu ergreifen sind, um die gesetzlichen Regelungen in der Praxis durchzusetzen, wird den einzelnen Mitgliedsstaaten überlassen.

Weiterhin werden die Mitgliedsstaaten aufgefordert, auch Schutzmaßnahmen für juristische Personen wie Unternehmen oder öffentlichen Einrichtungen vor unerwünschten Massensendungen zu treffen. Hier liegt es an den Mitgliedsstaaten, ob sie sich für eine Opt-in- oder Opt-out-Regelung entscheiden.

Der materiell größte Unterschied zwischen beiden EU-Richtlinien bezüglich Anti-Spam-Maßnahmen ist, dass in der E-Commerce-Richtlinie (2000) mindestens ein Opt-out-Verfahren, in der Datenschutzrichtlinie (2002) aber bereits das stärker den Nutzer schützende Opt-in-Verfahren für natürliche Personen vorgeschrieben wird. Damit reagierte die EU-Kommission auf das innerhalb sehr kurzer Zeit stark angewachsene Spam-Aufkommen.

---

63 Vgl. Gutsche (2003), S. 46f.

64 Richtlinie 2002/58/EG des Europäischen Parlamentes und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation („Datenschutzrichtlinie für elektronische Kommunikation“).

65 Vgl. Artikel 13 EU-Richtlinie 2002/58/EG.

Kritik an den aktuellen EU-Vorschriften zum Spamming wird dahingehend geübt, das natürliche Personen, die nicht selbst Teilnehmer (Subscriber) sind, nicht unter den Schutz der Opt-in-Regelung fallen.[66] Somit sind beispielsweise Familienmitglieder mit eigener E-Mail-Adresse, aber ohne eigene Vertragsbeziehung zum ISP oder Mitarbeiter in Unternehmen mit persönlicher E-Mail-Adresse weniger gut vor Spam geschützt.

In einer Mitteilung vom 22.01.2004 betont die Kommission noch einmal die Bedeutung des Kampfes gegen Spam und kündigte weitere Vorkehrungen an, um Spammer rechtlich verfolgen zu können.[67] Eine damit zusammenhängende Maßnahme ist das

Contact Network of Spam Enforcement Authorities (CNSA)

Anti-Spam Behörden aus 13 europäischen Ländern haben auf Initiative der EU ein Kontakt-Netzwerk gegründet, um die Strafverfolgung von Spammern innerhalb der EU zu erleichtern. Weitere Länder sollen der Initiative künftig beitreten. Die CNSA arbeitet mit ähnlichen Initiativen der OECD und der ITU zusammen.

Mitglieder sind die belgische Kommission zum Schutz der Privatsphäre und der belgische Föderale Öffentliche Dienst Wirtschaft – Generaldirektion Durchsitzung und Vermittlung, der dänische Verbraucherschutzdienst (Ombudsman), die französische Datenschutzbehörde CNIL, die griechische Datenschutzbehörde, das irische Ministerium für Kommunikation, Meeres- und Naturressourcen und das Amt des irischen Datenschutzbeauftragten, die italienische Datenschutzbehörde, die litauische Datenschutzbehörde, das Amt des maltesischen Datenschutzbeauftragten, die Regulierungsbehörde für elektronische Kommunikation (OPTA) und die Datenschutzbehörde (CBP) der Niederlande, das österreichische Bundesministerium für Verkehr, Innovation und Technologie, die spanische Datenschutzbehörde, die tschechische Datenschutzbehörde und das Amt des zypriotischen Datenschutzbeauftragten.

Deutsche Kontaktstellen sind der Eco-Verband in seiner Funktion als Hotline der Anti-Spam Task Force[68] und für Rufnummernspam die Bundesnetzagentur.

Spotspam-Projekt

Spotspam ist ein europäisches Projekt im Rahmen des EU Safer Internet Action Plan. Beteiligt sind u.a. der deutsche Eco-Verband und die polnische Internet-Organisation NASK. Die europäische Internetorganisation EuroISPA und der Londoner Internet-Exchange LINX sind ebenfalls involviert. Durch Spotspam soll die Verfolgung von Spammern europaweit vereinfacht werden, indem Beschwerden aus verschiedenen

---

66 Vgl. Asscher/van Erve (2004), S. 38f.
67 Communication on unsolicited commercial communications or ‘spam’ COM(2004) 28 final, Brussels, 22.01.2004.
68 Erläuterung erfolgt im Kapitel „Selbstregulierung“.

Ländern zentral gesammelt und Adressen von Hotlines bzw. Spambox-Projekten zusammengeführt werden.

7.1.4 London Action Plan (LAP)

Die Handelsbehörden aus Großbritannien und den USA, das UK´s Office of Fair Trading (OFT) und die US Federal Trade Commission organisierten im Oktober 2004 einen Anti-Spam-Workshop, aus dem eine internationale Zusammenarbeit zur Spam-Bekämpfung hervorging. Schließlich unterzeichneten zuständige Behörden und Organsationen aus 15 Ländern den „London Action Plan“. Die Initiative ist offen für öffentliche und private Anti-Spam-Organisationen.

Mitglieder sind die Australian Communications & Media Authority (ACA), Australian Competition and Consumer Commission (ACCC); Office of the Privacy Commissioner of Canada, National Consumer Service (SERNAC), Chile; Union Network Beijing, China; der dänische Verbraucher-Ombudsman; die finnische Verbraucherschutzbehörde, die irische Datenschutzbehörde, das japanische Ministry of Internal Affairs and Communications, Telecommunications Bureau, Telecommunications Business Department, Telecommunications Consumer Policy Division und die Japan Fair Trade Commission (JFTC); die litauische Regulierungsbehörde für Kommunikation; das National ICT Security and Emergency Response Centre (NISER), Malaysia; Procuraduria Federal del Consumidor, Comision Federal de Telecomunicaciones, Mexiko; Korean Information Security Agency (KISA) und Korea Consumer Protection Board, die spanische Datenschutzbehörde, der schwedische Consumer Agency/Consumer Ombudsman, das Schweizer State Secretariat for Economic Affairs – SECO, die niederländische Regulierungsbehörde Opta, das Office of Fair Trading und der Information Commissioner Office (ICO), UK sowie die US Federal Trade Commission.

Teilnehmer aus der Industrie sind Telefonica, Belgien; Santiago Chamber of Commerce, Chile; Internet Society of China; Microsoft EMEA, Frankreich; Eco, Deutschland; Outblaze Limited, Hongkong; Microsoft EMEA UK, LINX, ISPA UK, Nominet UK, Wanadoo UK plc; Latham & Watkins LLP (für AOL).

Ähnlich wie die Initiativen der ITU und OECD hat auch der London Action Plan zum Ziel, Kooperationen zwischen den zuständigen Behörden zu fördern und eine verbesserte Strafverfolgung zu erreichen. Besonders wichtig ist den Initiatoren dabei die Zusammenarbeit zwischen öffentlichen und privaten Akteuren.

7.2 Gesetze und regulatorische Maßnahmen

7.2.1 Rechtslage in Deutschland

Die Umsetzung des Artikels 13 der Datenschutzrichtlinie für elektronische Kommunikation erfolgte in Deutschland im Rahmen der Neufassung des Gesetzes gegen den unlauteren Wettbewerb (UWG) vom 3. Juli 2004. In § 7 UWG werden Handlungen, die einen Marktteilnehmer unzumutbar belästigen für unlauter nach § 3 UWG und damit für unzulässig erklärt. § 7 UWG schreibt die bisherige Rechtsprechung gesetzlich fest und setzt der Direktwerbung enge rechtliche Grenzen. Betroffen sind davon alle Formen der Direktwerbung über Kommunikationsnetze, d. h. alle unerwünschten Kontaktaufnahmen mittels Telefon, Fax, E-Mail, SMS oder sonstiger elektronischer Kommunikationsdienste. Dabei muss es sich bei einer unzumutbaren Belästigung von Marktteilnehmern im Sinne des § 7 UWG nicht um Werbung im engeren Sinne handeln. Auch eine Aufforderung, über eine Premiumrate-Rufnummer eine Meinungsäußerung abzugeben, fällt beispielsweise unter diese Vorschrift.[69]

Konkret setzt § 7 Abs. 2 UWG der Direktwerbung die folgenden Grenzen:

- Telefonwerbung ist gegenüber Verbrauchern nur beim Vorliegen einer Einwilligung zulässig. Gewerbetreibende dürfen hingegen bereits bei einer mutmaßlichen Einwilligung für Werbezwecke angerufen werden. Eine mutmaßliche Einwilligung ist nach der Rechtsprechung dann anzunehmen, wenn ein sachliches Interesse am Erhalt der Werbung auf Grund konkreter Umstände vermutet werden kann sowie nur das Kommunikationsmedium Telefon geeignet erscheint, diese Werbung zu übermitteln.

- Fax- und E-Mail-Werbung darf nur dann gesendet werden, wenn der Adressat eine ausdrückliche Einwilligung gegeben hat (Opt-in-Verfahren). Gleiches gilt für Werbeanrufe von automatischen Anrufmaschinen. Dabei ist es unerheblich, ob der Adressat eine natürliche oder juristische Person ist. Hier geht also das deutsche Recht über die Europäische Datenschutzrichtlinie hinaus und bezieht auch Empfänger in den Unternehmen in das Opt-in-Verfahren mit ein.

- Bei E-Mail-Werbung besteht allerdings die Ausnahme, dass eine E-Mail-Adresse, die ein Unternehmer durch den Verkauf von Waren oder Dienstleistungen erhalten hat, für die Bewerbung ähnlicher Angebote genutzt werden darf, es sei denn, der Kunde hat der Verwendung widersprochen (Opt-out-Verfahren). Zudem muss der Werbende darauf hinweisen, dass der Empfänger dieser Werbung jederzeit widersprechen kann.

---

69 Vgl. Kaestner/Tews (2004), S. 118ff.

Die Beweislast für das Einverständnis der E-Mail-Werbung liegt nach einem Urteil des BGH vom 11.3.2004 beim Werbenden.[70] Um dieser Anforderung besser gerecht zu werden und um zu vermeiden, dass Dritte missbräuchlicherweise das Einverständnis für eine fremde E-Mail-Adresse abgeben können, wird in der Praxis zumeist auf das doppelte Opt-in-Verfahren zurückgegriffen. Hierbei wird vom Werbenden zunächst eine Rückfrage an die betreffende E-Mail-Adresse geschickt. Diese Rückfrage enthält entweder einen Bestätigungslink oder die Aufforderung zu antworten. Erst danach gilt die Einwilligung als bestätigt und wird wirksam.

- Unlauter sind alle Werbeaussendungen, bei denen die Identität des Absenders verschleiert oder verheimlicht wird oder die keine gültige Adresse enthalten, an die der Empfänger sein Opt-out richten kann. Gleiches gilt für Werbeaussendungen, bei denen lediglich eine Premiumrate-Rufnummer angegeben wird.

Rechtsfolgen von Wettbewerbsverstößen nach § 7 UWG können der Anspruch auf Unterlassung und Schadenersatz sowie eine Gewinnabschöpfung sein. Voraussetzung für jegliches gerichtliches Vorgehen ist jedoch, dass der Verursacher der unerwünschten Sendung zu ermitteln ist.

Klageberechtigt auf Grund der UWG-Bestimmungen sind allerdings nicht die Empfänger von unerwünschten Massensendungen, sondern die Mitbewerber des Versenders sowie Verbände, wie Verbraucherverbände oder die Zentrale zur Bekämpfung unlauteren Wettbewerbs.

Die Empfänger unerwünschter Massensendungen besitzen im Regelfall nur eine Klagemöglichkeit auf Schadensersatz nach dem BGB. Privatpersonen können sich dabei auf die Verletzung des allgemeinen Persönlichkeitsrechts und Gewerbetreibende auf die Verletzung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb berufen und im Rahmen der §§ 823 BGB, 1004 BGB klagen.

In besonderen Fällen kann auch das Strafrecht gegen unerwünschte Massensendungen herangezogen werden, was im Falle einer Verurteilung weitaus drastischere Konsequenzen nach sich zieht. Strafrechtsnormen sind dann einschlägig, wenn eine Strafbarkeit bei den Inhalten der unerwünschten Massensendungen gegeben ist.

Strafbar auf Grund der Inhalte sind beispielsweise unerwünschte Massensendungen mit pornografischen Abbildungen, die nach § 184 StGB mit Freiheitsstrafe bis zu einem Jahr oder Geldstrafe zu ahnden sind. Ebenfalls können die Inhalte die Straftatbestände Betrug (§ 263 StGB), Beleidigung oder Verleumdung (§§ 185ff) oder unerlaubtes Glücksspiel (§ 284 StGB) enthalten.

---

70 Vgl. BGH, Urteil vom 11.3.2004, ger. Az.: -I ZR 81/01.

Eine Strafbarkeit der in unerwünschten Massensendungen üblicherweise gefälschten Absenderangaben ist hingegen bei Spam-E-Mails, unerwünschten Automatenanrufen oder SMS nicht gegeben, da diese Nachrichten ohne eine digitale Signatur auch keine Urkundeneigenschaft besitzen. Die Strafrechtsparagrafen § 269 StGB (Fälschung beweiserheblicher Daten) und § 267 StGB (Urkundenfälschung) kommen daher nicht zur Anwendung.

Die Fälschung der Absenderadresse ist derzeit nur dann strafbar, wenn eine eingetragene Marke oder ein Geschäftskennzeichen als Absender eingesetzt wird. Hierdurch wird gegen § 143 des Gesetzes über den Schutz von Marken und sonstigen Kennzeichen (MarkenG) verstoßen, was bei gewerbsmäßig agierenden Massenversendern mit Freiheitsstrafe von bis zu 5 Jahren geahndet wird.

7.2.2 Praxis der Gesetzesanwendung

Ein grundsätzliches Problem beim Vorgehen gegen unerwünschte Massensendungen ist, dass die Belästigung und die Kostenverursachung auf Empfängerseite jeder einzelnen Aussendung nur marginal sind. Erst die große Menge dieser, gegenwärtig hauptsächlich in Form von E-Mails versandten Nachrichten und ihre Relation zur erwünschten elektronischen Post lassen das Problem entstehen. Das Vorgehen gegen einen Spam-Versender ist für den einzelnen Empfänger nur von sehr geringem Nutzen, da die Belästigung durch alle weiteren unerwünschten Massensendungen weiterhin besteht.

Gleichzeitig ist ein wirksames Vorgehen gegen einen Absender unerwünschter Massensendungen mit erheblichem Aufwand verbunden, denn die überwiegende Mehrzahl der unerwünschten Nachrichten von mehr als 95 Prozent wird von Absendern im Ausland verschickt. Da bei den Anti-Spam-Gesetzen das Ursprungslandprinzip gilt, können die deutschen Gesetze nicht auf ausländische Absender angewendet werden. Um gegen die Absender im Ausland vorzugehen, müssen die Empfänger von unerwünschten Massensendungen zunächst das Herkunftsland ermitteln, um die dortige Rechtslage zu prüfen.

Bestehen auf Basis der jeweiligen Rechtslage im Herkunftsland Möglichkeiten, gegen den Absender vorzugehen, so muss dieser außerdem zweifelsfrei identifiziert werden. Erschwert wird die Ermittlung des Absenders und seines Standortes jedoch durch zahlreich genutzte Verschleierungstaktiken. So können beispielsweise bei E-Mails beliebige Absenderadressen eingesetzt werden. Auch die schwer zu fälschende Absender-IP-Adresse führt nicht unbedingt zum Verursacher, denn ein Großteil der zirkulierenden Spam-Mails wird über Malware wie Trojaner gesteuert von Zombie-PCs versendet, deren Besitzer ahnungslos und unbeteiligt sind. Bei Automatenanrufen kann die Anrufernummer unterdrückt sein und auch bei SMS bestehen Möglichkeiten die Absendernummer zu fälschen oder zu unterdrücken.

Die Ermittlung des Absenders, die Information über die Gesetzeslage im Absenderland sowie das Einleiten rechtlicher Schritte gegen den Verursacher der unerwünschten Sendung sind mit ganz erheblichen Informations- und Transaktionskosten verbunden. Entsprechend sind die Anreize für einen Empfänger unerwünschter Massensendungen direkt gegen die Verursacher vorzugehen nur äußerst gering. Zumal dieser hohe Aufwand keine oder nur marginalen Einfluss auf den Empfang weiterer unerwünschter Mails von anderen Absendern besitzt.

Vor dem Hintergrund dieser ungünstigen Anreizsituation entspricht es der wirtschaftlichen Rationalität der Empfänger, lediglich in Abwehrmaßnahmen wie automatische Filter für unerwünschte E-Mails zu investieren, nicht jedoch in die Ermittlung der Absender, um den Rechtsweg nach jeweiligem Landesrecht zu beschreiten. Im Falle von deutschen Absenderadressen wären dies zivilrechtliche Klagen zur Durchsetzung der oben skizzierten Unterlassungs- und Schadensersatzansprüche nach dem UWG bzw. dem BGB.

Zudem ist ein gewisser Gewöhnungseffekt, zumindest was E-Mail-Spam betrifft, erkennbar. In regelmäßig durchgeführten Umfragen unter US-Internetnutzern hat sich gezeigt, dass trotz objektiv messbarer Zunahme von Spam, die subjektiv wahrgenommene Beeinträchtigung der Nutzer leicht zurückgeht.[71] Dieser Gewöhnungseffekt senkt die Bereitschaft zur Aufnahme von rechtlichen Schritten gegen unerwünschte Massensendungen zusätzlich.

Rufnummern-Spamming

Eine weitaus bessere Ausgangssituation besteht bei der Gesetzesanwendung im Zusammenhang mit unerwünschten Massensendungen, die Rufnummern enthalten, dem Rufnummern-Spamming. Das Geschäftsmodell der Absender dieser Art von unerwünschten Massensendungen beruht im Regelfall auf der Nutzung von Premiumrate-Rufnummern. Da gegenwärtig in Deutschland ausschließlich deutsche Premiumrate-Rufnummern erreichbar sein sollten, besteht die Möglichkeit missbräuchlich eingesetzte Nummern durch Anordnung der Bundesnetzagentur zu sperren. Allerdings trifft dies nicht auf ausländische Nummern zu, die missbräuchlich als Premiumrate-Rufnummern genutzt werden.

Auf Grundlage von § 67 TKG, 2003 durch das Gesetz zur Bekämpfung des Missbrauchs mit 0190er-/0900er-Mehrwertdiensterufnummern eingeführt, hat die Bundesnetzagentur die Befugnis und bei Vorliegen von gesicherten Erkenntnissen die Möglichkeit und auch die Pflicht, die Abschaltung der missbräuchlich genutzten Rufnummern anzuordnen. Weiterhin müssen Tatsachen, die den Verdacht einer Straftat oder einer

---

71 Vgl. PEW Internet & American Life Project (2005). Gemessen wurde die subjektive Beeinträchtigung durch Spam mit den Fragen, ob durch Spam die Nutzung von Internet reduziert wurde, ob durch Spam das Vertrauen in das Internet verloren wurde sowie ob durch Spam die Internetnutzung unangenehm wurde.

Ordnungswidrigkeit begründen, nach § 67 (3) TKG der Staatsanwaltschaft oder der Verwaltungsbehörde mitgeteilt werden.

Voraussetzung für das Tätigwerden der Bundesnetzagentur ist eine schriftliche Beschwerde des Empfängers der unerwünschten Sendung sowie deren Rechtswidrigkeit, also beispielsweise der Verstoß gegen § 7 UWG. Als konkrete Maßnahmen spricht die Bundesnetzagentur in diesen Fällen zunächst eine Abmahnung aus und leitet ein Anhörungsverfahren bei den Netzbetreibern ein.[72] Kann der Verdacht nicht ausgeräumt werden, so folgt die Anordnung der Abschaltung der Rufnummer gegenüber dem Netzbetreiber. Auf diese Weise wird den Versendern der unerwünschten Massensendungen das Geschäftsmodell entzogen. Zum Teil schalten die Netzbetreiber die betroffenen Nummern bereits freiwillig im Rahmen des Anhörungsverfahrens ab.

Die Maßnahmen der Bundesnetzagentur besitzen eine hohe Effektivität, da sie in der Regel als Verwaltungsakte sofort vollziehbar sind. Die Adressaten, d.h. die Netzbetreiber, können Widerspruch einlegen. Da die Netzbetreiber jedoch zum Schutz der seriösen Premiumrate-Diensteanbieter ebenso an Maßnahmen gegen Rufnummernmissbrauch Interesse haben, sind Widersprüche von Netzbetreibern selten. Die Absender der unerwünschten Massenaussendungen können sich als Betroffene der Maßnahme im Wege des einstweiligen Rechtsschutzes oder mittels Klage vor dem Verwaltungsgericht gegen die Maßnahme wehren. Diese Verfahren können sehr zeitintensiv und aufwändig – nicht zuletzt für die BNetzA – sein.

Seit die Bundesnetzagentur gegen unerwünschte Massenaussendungen vorgeht, hat bislang ein Betroffener eine Klage vor dem Verwaltungsgericht gegen eine Unterlassungsverfügung der BNetzA wegen Telefon-Spam angestrengt. Diese Klage wurde jedoch rechtskräftig abgewiesen, womit die Maßnahmen der Bundesnetzagentur gegen Spamming in Verbindung mit Rufnummernmissbrauch gerichtlich bestätigt wurden.[73]

7.3 Selbstregulierung

Der Erkenntnis folgend, dass gesetzliche und regulatorische Maßnahmen bei der Bekämpfung von unerwünschten Massenaussendungen das unverzichtbare rechtliche Fundament bilden, darüber hinaus jedoch weitere Maßnahmen der beteiligten Akteure erforderlich sind, sind die Unternehmen der Internetwirtschaft darum bestrebt, neben individuellen Filtermaßnahmen auch organisatorische Vereinbarungen untereinander zu treffen und selbstregulativ tätig zu werden.

Hauptmotivation aller Beteiligten ist, die durch unerwünschte Massenaussendungen stark steigenden Transaktionskosten bei der Nutzung der elektronischen Kommuni-

---

72 Vgl. www.regtp.de/aktuelles/start/fs_03.html.
73 Vgl. RegTP News 01/2005, S. 4f.

kationsdienste zu begrenzen bzw. zu senken. Daneben besitzen die unterschiedlichen Anbietergruppen spezifische Interessen.

7.3.1 Interessen der Anbietergruppen

ISP

Für die Internet Service Provider und die Anbieter von E-Mail-Diensten stellt das enorm hohe Spamaufkommen zunächst einen gewichtigen Kostenfaktor durch zusätzlichen Traffic und Speicherplatz dar und wirkt sich daher je nach Wettbewerbssituation negativ auf die Preise der Dienste oder auf die Rendite der Unternehmen aus. Darüber hinaus besteht jedoch auch die Gefahr, dass die Nutzer ihr Vertrauen in E-Mail als zuverlässiges und effizientes Kommunikationsmedium verlieren und nachhaltig weniger E-Mail-Dienste nachfragen.

Das Interesse der ISP besteht deshalb darin, die Kosten der Übertragung und Speicherung von unerwünschten Massenaussendungen zu vermeiden sowie ihre Kunden vor diesen Aussendungen zu schützen und damit die Qualität ihrer Dienste zu sichern. Ein wirksamer Schutz vor unerwünschten Massensendungen kann mitunter als Differenzierungsmerkmal im Qualitätswettbewerb eingesetzt werden.

Zudem werden die entgeltfreien Angebote der ISP im großen Umfang von den Versendern unerwünschter Massenaussendungen für deren Verschickungen missbraucht.[74] Für diese E-Mail-Dienste entsteht hierdurch nicht nur ein Imageverlust sondern sie laufen auch Gefahr, von anderen Mailprovidern als Spamquelle global gesperrt zu werden, so dass auch die E-Mails aller anderen Nutzer dieser Domain ausgefiltert werden.

Anbieter von Telefondiensten

Im Bereich der Telefondienste stellen unerwünschte Massensendungen bislang im Vergleich zu E-Mail ein quantitativ weit selteneres Phänomen dar. Einer der wichtigsten Gründe hierfür ist, dass für Festnetz- und Mobilanrufe sowie für das Versenden von SMS Entgelte anfallen, die wiederum die meisten Spamming-Geschäftsmodelle unrentabel erscheinen lassen. Gleichzeitig stellt aber ein unerwünschter Anruf einer Anrufmaschine oder eine SMS eine deutlich größere Störung dar als der Eingang von Spam in das E-Mail-Postfach, so dass die Toleranzgrenze der Telefonkunden bei unerwünschten Anrufen und SMS schon sehr viel früher erreicht sein dürfte.

Insofern liegt für Telefondiensteanbieter das Hauptproblem von unerwünschten Massensendungen weniger in den Kosten durch zusätzlichen Verkehr auf den Netzen als

---

74 Eine Auswertung von mehreren 100 Millionen Spam-Mails im März 2005 durch die Softwarefirma Commtouch hat ergeben, dass die unerwünschten Massenaussendungen zu 11,4% von yahoo.com, zu 5,5% von hotmail.com und zu 4,5% von msn.com kostenlosen E-Mailkonten verschickt werden.

vielmehr in der Beeinträchtigung der Nutzer und deren gefährdetes Vertrauen in den Dienst.

Mit der zunehmenden Nutzung von Voice-over-IP-Diensten und einem deutlichen Rückgang der Entgelte für (internationale) Anrufe ist für die Zukunft ein starker Anstieg von Spit zu befürchten. Die Anbieter von VoIP-Diensten sehen sich mit dem Risiko konfrontiert, dass ihr Dienst durch Spit schweren Imageschaden nimmt und die prognostizierten Wachstumsraten ausbleiben. Insbesondere bei der Zusammenschaltung von Voice-over-IP-Netzen mehrerer Anbieter und dem Angebot entgeltfreier Interngespräche innerhalb der zusammengeschalteten Netze müssen sich die VoIP-Anbieter darauf verlassen können, dass Spit-Versender von allen Netzbetreibern der Kooperation zuverlässig identifiziert und gesperrt werden.

Direktwerber

Unternehmen, die seriöse Direktwerbung über elektronische Kommunikationsnetze in ihren Marketing-Mix integrieren und die die gesetzlichen Vorgaben aus dem UWG einhalten, sehen diese Kommunikationskanäle durch unerwünschte Massensendungen immer stärker bedroht.

Zum einen besteht eine hohe Wahrscheinlichkeit, dass auch seriöse und legale Werbeaussendungen irrtümlich von Spamfiltern aussortiert werden und den Empfänger nicht erreichen. Zum anderen verkleinert die Flut an unerwünschten Massenmails die generelle Akzeptanz der Empfänger für das Direktmarketing über elektronische Kommunikationsnetze, so dass dieses Marketinginstrument nachhaltig beschädigt werden könnte.

Markeninhaber

Der Großteil der unerwünschten Massensendungen wird zur Werbung für unseriöse Produkte genutzt. Zu den am meisten durch Spam beworbenen Produkten zählen Arzneimittel und hier insbesondere das Potenzmittel Viagra, sowie Finanzprodukte.[75] Bei den beworbenen Medikamenten handelt es sich zumeist entweder um Generika, deren Qualität äußerst fragwürdig erscheint oder sogar um nicht zugelassene Medikamente und Drogen.

Das US-Pharmaunternehmen Pfizer als Markeninhaber von Viagra sieht durch die hohe Anzahl von unerwünschten Massenaussendungen, die für Viagra-Generika werben und

---

75 Eine Auswertung von mehreren 100 Millionen Spam-Mails im März 2005 durch die Softwarefirma Commtouch ergab 22,4% Medikamentenwerbung, 10,4% Finanzbetrug, 9,62% Viagra Werbung, 9,14% Werbung für Hypothekenfinanzierungen, 6,87% Softwareangebote und 6,65% pornografische Angebote. Vgl. http://www.commtouch.com//Site/News_Events/pr_content.asp?news_ id=346&cat_ id=1

deren Anwendung als potenziell gefährlich eingeschätzt wird, den Ruf seines Markenproduktes ernsthaft gefährdet.[76]

Unternehmen, deren Marken gefälscht und über unerwünschte Massenmails beworben werden, besitzen ein starkes Interesse gegen die Absender vorzugehen. Sie stoßen jedoch bei der Identifizierung der Absender und des Absendeortes auf die gleichen Schwierigkeiten wie die Empfänger.

7.3.2 Beispiele für konkrete Maßnahmen

Um die Flut unerwünschter Massenaussendungen insbesondere per E-Mail einzudämmen und dabei gleichzeitig die Qualität des Kommunikationsmediums aufrechtzuerhalten, unternehmen die Akteure auf der Anbieterseite zahlreiche organisatorische und selbstregulative Anstrengungen.

Hotline

Seit mehreren Jahren betreibt Eco eine Internet-Hotline zur Entgegennahme von Beschwerden über illegale und schädigende Internetinhalte. Um Beschwerden zu allen Aspekten von Gesetzesverstößen, die den Diensten World Wide Web, E-Mail, Tauschbörsen und Peer-to-Peer, Chats, Newsgroups, Diskussionsforen, mobile Inhalte sowie sonstigen Diensten zuzuordnen sind, zentral entgegenzunehmen, betreibt Eco in Kooperation mit der Freiwilligen Selbstkontrolle Multimedia-Diensteanbieter (FSM) die Site „Internet-Beschwerdestelle.de“.

Certified Senders Alliance von Eco und DDV

Als selbstregulative Maßnahme haben die Direktmarketing betreibenden Unternehmen und die Unternehmen der Internetwirtschaft, vertreten durch Eco und den Deutschen Direktmarketing Verband (DDV), im Herbst 2004 mit der Certified Senders Alliance ein Projekt für eine zentralisierte Positivliste (auch „Whitelist“ genannt) gestartet.[77]

Unternehmen, die seriöses und gesetzeskonformes Direktmarketing betreiben, treten zunehmend an einzelne ISP heran und bitten um die Aufnahme in deren Positivliste, um zu vermeiden, dass ihre Newsletter und sonstigen Massensendungen durch die automatischen Spamfilter aussortiert werden. Dabei entstehen für beide Seiten erhebliche Transaktionskosten durch die Verhandlung sowie die Überprüfung der Kriterien für einen Eintrag in die Positivliste. Die Direktmarketingunternehmen müssen mit zahlreichen ISP verhandeln und deren jeweilige Kriterien für eine Positivlisteneintragung erfül-

---

76 Vgl. „Pfizer and Microsoft Target Sellers of Illegal Viagra and International Spam Rings“, http://www.pfizer.com/are/news_releases/2005pr/mn_2005_0210.html

77 Vgl. http://www.eco.de/servlet/PB/menu/1446034_l1/index.html.

len. Umgekehrt müssen die ISP eine hohe Anzahl von Anfragen von Unternehmen zur Aufnahme in ihre Positivliste bearbeiten.

Um diese kostspieligen multilateralen Verhandlungen zu vermeiden, wurde in der Certified Senders Alliance ein Code of Conduct für Massenversender ausgearbeitet. Nur Massenversender, die diese Kriterien einhalten werden von der CSA zertifiziert und in die zentralisierte Positivliste aufgenommen.[78] Die teilnehmenden ISP verpflichten sich zur Anwendung dieser Positivliste.[79] Für die ISP ist die Übernahme der CSA-Liste kostenfrei, während für die Massenversender sowohl Anmelde- als auch laufende Entgelte anfallen.

Die standardisierten Verfahren und die zentralisierten Ansprechpartner versprechen eine höhere Effizienz. Zudem dient die CSA als Beschwerdeinstanz, sollte einer der Teilnehmer gegen den Code of Conduct bzw. gegen die Anwendung der Positivliste verstoßen.

Aktionsbündnis gegen Spam

Im März 2005 schlossen der Verbraucherzentrale Bundesverband (VZBV), die Zentrale zur Bekämpfung unlauteren Wettbewerbs (WBZ) und Eco ein Aktionsbündnis gegen Versender unerwünschter Massensendungen per E-Mail. Intendiert ist ein rechtliches Vorgehen gegen die Verstöße nach § 7 UWG.

Im Aktionsbündnis werden komplementäre Kompetenzen und Fähigkeiten gebündelt: Die Internetunternehmen besitzen das Know-how die oftmals verschleierten Absender zurückzuverfolgen und zu identifizieren, können aber nach § 7 UWG keine juristischen Schritte gegen die Absender einleiten. Die Verbraucherschützer hingegen können durch das Instrument der Verbandsklage aktiv werden, wenn sie Kenntnis über die Absender unerwünschter Massensendungen haben.

Allerdings kann auf Grund der nationalen Gesetzgebung nur gegen Spam-Versender und deren Auftraggeber in Deutschland vorgegangen werden, was die Wirksamkeit des Vorhabens einschränkt. Gleichzeitig ist jedoch auf anderen Ebenen (EU, London Action Plan) eine internationale Zusammenarbeit intendiert, so dass auch die Strafverfolgung von Spam aus dem Ausland in Zukunft besser gewährleistet ist.

Verbandsklagerecht nach UWG

Das novelliert UWG sieht ein Verbandsklagerecht vor, das die deutschen Verbände VZBV, Eco und Wettbewerbszentrale im Rahmen ihres Aktionsbündnisses in Bezug auf Spam systematisch nutzen. Eco leitet Beschwerden über die eigene Hotline an den

---

78 Bis April 2005 wurden die Massenversender Agnitas, eCircle, inxmail, promio.net und mailprofiler durch CSA zertifiziert.

79 Bis April 2005 haben die ISP Arcor, Freenet, GMX, Schlund + Partner sowie 1&1 ihre Teilnahme vertraglich vereinbart.

VZBV (Beschwerden privater Verbraucher) und an die Wettbewerbszentrale (Beschwerden von Unternehmen/Arbeitnehmern) weiter. Betroffene wenden sich auch in großer Zahl direkt an diese Beschwerdestellen. Beim VZBV gehen nach Angaben des Verbandes täglich 7.000 bis 8.000 Beschwerde-Mails ein. Je bekannter die Beschwerdestellen werden, umso stärker steigt diese Anzahl voraussichtlich an.

Das Ziel der Verbände, durch strafbewehrte Unterlassungserklärungen die Spam-Flut zu vermindern, zeitigt erste Erfolge. Zwar unterzeichnen die Spammer nicht in jedem Fall die Erklärungen, sie unterlassen in der Regel aber den Versand unerwünschter Massen-Mails. Außerdem werden Klagen vorbereitet und in internationaler Zusammenarbeit versucht, Spammern, die organisiert weltweit tätig sind, strafrechtlich zu verfolgen. Aus Sicht der Verbände mangelt es dazu in Deutschland noch an wirksamen Sanktionen, die ausreichend abschreckend wirken und einer zentralen Anlaufstelle, an die sich Institutionen aus dem Ausland wenden können, wenn es um die Verfolgung von Spammern geht.

7.4 Technische Maßnahmen

Da das Problem unerwünschter Massensendungen bislang vor allem beim E-Mail-Dienst bedrohliche Ausmaße angenommen hat, werden hier bereits zahlreiche technische Maßnahmen eingesetzt, um Spam-Mails automatisch auszusortieren.

Praktisch alle E-Mail-Dienstleister sowie ein Großteil der Organisationen mit eigenem Mailserver überprüfen die eingehenden E-Mails, um unerwünschte Mails direkt am Mail-Server (MTA) zurückzuweisen bzw. auszusortieren. Hinzu kommen Spamfilter, die nachgelagert in die E-Mail-Clients integriert sind.

Die grundsätzlichen Schwierigkeiten bei der automatisierten Spamfilterung liegen zum einen darin, dass die Versender ihre unerwünschten E-Mails permanent auf die Filterungskriterien einstellen, um eine Aussortierung zu umgehen. Zum anderen sind die Merkmale für Spam nicht vollständig objektivierbar. Ein Newsletter eines Direktmarketingunternehmens kann beispielsweise - je nach vorherigem Einverständnis des Empfängers - eine erwünschte oder eine unerwünschte E-Mail darstellen.

Technische Maßnahmen, selbst wenn sie noch so aufwändig und ausgefeilt gestaltet sind, können somit keinen 100%igen Schutz vor Spam-Mails bieten. Allerdings sorgt die Filterung eines Großteils der unerwünschten Mails angesichts des enormen Spam-Aufkommens für eine Aufrechterhaltung der Dienstequalität von E-Mail.

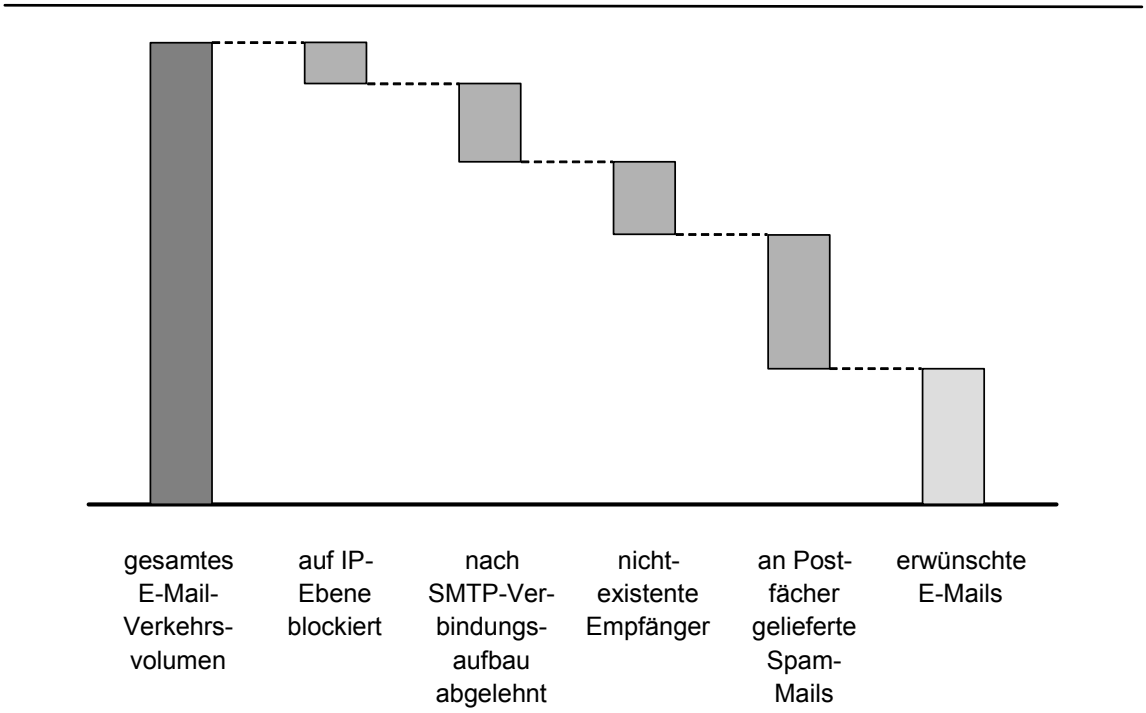
Bei den falschen Sortierungen durch die technischen Maßnahmen unterscheidet man zwischen den „False Negatives“, also den Spammails, die fälschlicherweise als erwünschte Nachrichten beurteilt werden und den „False Positives“, den erwünschten Nachrichten, die fälschlicherweise für Spam gehalten werden.

Idealerweise werden die Filter so eingestellt, dass die Rate der False Positives sehr gering ist, da die Nichtzustellung von erwünschten E-Mails die Verlässlichkeit des Kommunikationsmittels stark vermindert. Im Falle der False Negatives hingegen kann der Fehler durch einen Nutzereingriff relativ schnell beseitigt werden, so dass eine etwas höhere Rate an False Negatives tolerabel ist.

7.4.1 Überblick über die technischen Maßnahmen

Technische Maßnahmen gegen den Empfang von Spam-E-Mail setzen auf unterschiedlichen Ebenen an (vgl. Abbildung 7-2).[80] Solange die Authentisierung der Absender auf Grund des verwendeten Übertragungsprotokolls nicht möglich ist und in der weltweiten Anti-Spam-Gesetzgebung und Gesetzesanwendung weiße Flecken existieren, spielen technische Maßnahmen wie automatische Spamfilter eine wichtige Rolle bei der Bekämpfung unerwünschter Massenaussendungen.

Abbildung 7-2: Serielle Filterung von Spam-E-Mails



wik CONSULT

Quelle: IFIS

80 Vgl. Dietrich/Pohlmann (2004), S. 8ff.

IP-Ebene - Überprüfung der IP-Adresse des Absenders

- Abgleich mit Real-Time-Blacklists (RBL) und Open Relay Database (ORDB), die von verschiedenen Anbietern kommerziell oder kostenfrei bereitgestellt werden,
- z.T. Ausschluss von dynamisch zugewiesenen IP-Adressen (ISP-Dial-up-Adressen), da diese besonders häufig von Spammern genutzt werden,
- Mailserver-Authentifizierungsverfahren wie Sender Policy Framework (SPF), SenderID, Reverse MX, Designated Mailers Protocol (DMP), DomainKeys oder Identified Internet Mail,
- Messung der Frequenz der Zustellversuche, um IP-Adressen mit Spam-typischen Frequenzen aufzudecken.

SMTP-Ebene

- Überprüfung der HELO-Angaben,
- Abgleich der E-Mail-Adressen mit Black-, White- und Greylists,
- Überprüfung der Existenz der Empfänger-E-Mail-Adresse.

Inhalte-Ebene

- Analyse der Betreffzeile und des Inhalts auf Schlüsselwörter bzw. auf für Spam charakteristische Strukturen,
- Hash/Signatur Überprüfung,
- händische Filterung durch Personen.

In der Regel werden die unterschiedlichen technischen Maßnahmen kombiniert eingesetzt. Um das Risiko an False Positives zu minimieren und den Versendern die Anpassung ihrer Spam-Mails an die Filterkriterien zu erschweren, wird die Beurteilung meist mit Hilfe von Punkteverfahren für parallel bzw. nacheinander durchgeführte Tests vorgenommen.

7.4.2 IP-Adressen Datenbanken

Black- und Whitelists werden mittlerweile zahlreich und durch die unterschiedlichsten Organisationen und Unternehmen geführt und veröffentlicht. Zum Großteil stehen sie

kostenlos für automatisierte Abfragen bereit. Einige Listen werden auch ausschließlich proprietär von Anti-Spam-Dienstleistern geführt.[81]

Ein Einsatz von Black- und Whitelists zur Sortierung von E-Mails setzt voraus, dass die verwendeten Listen gewissenhaft und umfassend geführt werden. Für die Administratoren von E-Mail-Diensten ist es relativ schwierig, die Zuverlässigkeit und Qualität dieser Listen zu beurteilen.

Listen mit unvollständigen Einträgen werden zwar relativ schnell erkannt, da ihre Anwendung nicht zur effektiven Spamfilterung führt. Falsche Einträge hingegen, die zu False Positives und False Negatives führen, können von den Administratoren nicht so einfach aufgedeckt werden.

Falsche Einträge auf den Blacklists können mitunter bedeuten, dass alle E-Mails, die mit einer betroffenen IP-Adresse abgeschickt werden, ihre Adressaten nicht erreichen. Da bei E-Mail grundsätzlich keine Zustellbestätigungen erzeugt werden, erfährt der Absender zunächst nicht, dass seine Nachricht versehentlich als Spam aussortiert wurde.

Besteht ein begründeter Verdacht auf Löschung von E-Mails auf Grund von fälschlicherweise auf Blacklists aufgeführten IP-Adressen, so beginnt für den Geschädigten ein umständlicher und mit hohen Transaktionskosten verbundener Prozess, dies zu korrigieren. Zunächst muss herausgefunden werden, auf welchen Blacklists die IP-Adresse erscheint, um danach dem Verwalter der Liste glaubhaft darzulegen, dass von dieser keine Spam-Mails versendet worden sind.

Problematisch ist insbesondere, dass einige Blacklist-Betreiber IP-Adressen von vermeintlichen Spammern relativ ungeprüft in ihre Listen übernehmen. Gleichzeitig verlangen sie für deren Streichung von den jeweiligen Serverbetreibern Beweise, dass unter der betreffenden IP-Adresse kein Spam versendet wurde. Dieses Vorgehen ist sehr anfällig für Missbrauch. Zum einen können Unternehmen, die ihren Wettbewerbern schaden wollen, deren IP-Adressen recht einfach auf Blacklists setzen lassen. Zum anderen wurden bereits Fälle bekannt, in denen Blacklist-Betreiber zum Schutz vor falschen Einträgen auf eine kostenpflichtige Whitelist desselben Unternehmens verwiesen haben.[82]

Weniger gravierende Folgen haben falsche Einträge auf den Whitelists. Gelangen beispielsweise die IP-Adressen von Spam-Versendern auf eine Whitelist, so werden Spam-Mails zunächst fälschlicherweise nicht aussortiert, was aber unter Umständen durch nachgeschaltete Filter auf SMTP- oder Inhalte-Ebene geschieht. Zu viele Fehleinträge werden langfristig dazu führen, dass die jeweilige Whitelist nicht mehr konsultiert wird.

---

81 Eine unvollständige Zusammenstellung von Blacklists findet sich beispielsweise unter http://rbls.org/.

82 Vgl. „Hacker missbrauchen Spamblocklisten. Spamabwehr setzt oft auf das falsche Pferd“, VDI Nachrichten vom 22.4.2005.

Relativ unproblematisch sind Datenbanken, die Open Relay Mailserver auflisten, die einfach durch Spammer missbraucht werden könnten. In diesen Fällen kann durch deren Administratoren bewiesen werden, dass kein Open Relay mehr besteht.

7.4.3 Dynamische IP-Adressen

Um ihre Identität zu verschleiern, greifen Spamversender zuweilen auf dynamische IP-Adressen zurück, die bei der ISP-Einwahl zugewiesen werden. Auch Spam, der durch ahnungslose Internetnutzer verschickt wird, deren Rechner mit entsprechenden Viren, Würmern oder Trojaner infiziert sind, weist dynamische IP-Adressen auf. Im Jahr 2004 stammten nach Expertenschätzungen rund 30 bis 40 Prozent der Spammails von „Zombie-PCs“.[83]

Als recht erfolgreiche Gegenmaßnahme gegen die auf diesem Weg versendeten Spammails wird oftmals in den Mailsservern der Empfang von E-Mails mit IP-Adressen aus dem dynamisch zugewiesenen Adressenbereich der ISP gesperrt.

Diese Art der Spamfilterung ist für all jene seriösen Mailversender problematisch, die einen eigenen Mail Transfer Agent betreiben und einen Einwahlzugang zum Internet mit dynamisch zugewiesener IP-Adresse nutzen. Ihre Mails werden hierdurch ebenso blockiert. Das Problem kann jedoch relativ einfach umgangen werden, indem ein SMTP-Smarthost des ISP verwendet wird. Nicht betroffen sind Internetnutzer mit Einwahlzugang, die ihre E-Mail-Kommunikation über ein Konto bei einem E-Mail-Dienstleister abwickeln.

7.4.4 Mailserver-Authentifizierungsverfahren

Mailserver-Authentifizierungsverfahren sollen den Spam-Versendern unterbinden oder es ihnen zumindest erschweren, durch falsche Absenderangaben ihre Identität zu verschleiern (E-Mail-Spoofing). Sie sollen helfen, juristische Verfahren gegen diese Personen zu ermöglichen und somit dem Geschäftsmodell Spamming insgesamt die Basis zu entziehen.

Das E-Mail-Spoofing wird grundsätzlich dadurch ermöglicht, dass das E-Mail-Protokoll SMTP keine Authentifizierung erfordert, sondern die Möglichkeit vorsieht, unterschiedliche Absender- und Empfängeradressen im für die Adressierung notwendigen Envelope und im vom Nutzer lesbaren Header der E-Mail anzugeben. Zudem muss für eine erfolgreiche Zustellung im Envelope nur die Empfängeradresse korrekt sein, während die Absenderadresse falsch bzw. bewusst gefälscht sein kann.[84] Diese von den Autoren

---

83 Vgl. „Ferngesteuerte Spam-Armeen“, in c’t /04, S. 18.
84 vgl. „Wider die E-Mail-Massen. Neue Verfahren gegen Spam“, in c’t 15/2004.

des SMTP in guter Absicht vorgesehenen Möglichkeiten werden heute von Spammern vielfach missbraucht.

Bereits seit längerem wird über eine Erweiterung des SMTP um eine Authentifizierung diskutiert, um diese missbrauchsanfälligen Möglichkeiten auszuschalten. Im Kern geht es hierbei darum zu überprüfen, ob die im Mail-Envelope angegebene Absenderadresse autorisiert ist, über den Mailserver mit der angegebenen IP-Adresse E-Mails zu versenden. Diese Verknüpfung soll beispielsweise durch eine Ergänzung des Domain Name Systems (DNS) geschehen. Ein zusätzlicher Eintrag soll festlegen, für welche Domains von einer IP-Adresse E-Mails versandt werden dürfen (Reverse MX).

Die für Internet-Standards verantwortliche Internet Engineering Task Force (IETF) hat innerhalb mehrerer Arbeitsgruppen entsprechende Konzepte gesammelt. Es konnte sich jedoch bislang keines der vorgeschlagenen Verfahren, wie Sender Policy Framework (SPF), SenderID, RMX, DMP, DomainKeys oder Identified Internet Mail als allgemeiner Standard durchsetzen. Die Vorschläge zur Mailserver-Authentifizierung gehen mitunter mit Signaturverfahren einher, mit deren Hilfe die persönliche Absender-Authentifizierung gewährleistet werden soll.

Einer der größten Schwachpunkte von Authentifizierungs- und Signaturverfahren ist die Notwendigkeit von Datenbanken und Public-Key-Infrastrukturen. Die bislang weitgehend dezentral organisierte E-Mail-Abwicklung müsste künftig weitgehend zentralisiert werden.[85] Die Authentifizierungen würden über nur wenige Server weltweit abgewickelt, deren Betreiber eine beträchtliche Preissetzungsmacht und Kontrollmöglichkeiten hätten. Trotz des erheblichen Aufwands ist aber ungewiss, ob die Spammer diese Maßnahmen umgehen können, indem sie ihre Absenderadressen bei sog. Wegwerf-Domains, die nur für Spamming genutzt werden, registrieren lassen.

Ungelöst ist zudem die Frage, wie mit den Mails zu verfahren ist, die keine Authentifizierung besitzen. Sie könnten beispielsweise direkt auf IP-Ebene abgelehnt werden oder als potenzielle Spam-Mails markiert werden.

Authentifizierungsverfahren können nur dann zuverlässig gegen Spam funktionieren, wenn sie flächendeckend von allen Mailservern unterstützt werden. Bislang kommen sie lediglich in einigen Spamfiltern zum Einsatz, wobei die Authentifizierung nur als Hinweis und nicht als Beleg dafür gewertet wird, dass die jeweilige E-Mail nicht von einem Spammer stammt.

---

85 vgl. „Noch mehr Anti-Spam-Mittel und ihre Nebenwirkungen“, Heise-Online, v. 12.08.2004.

7.4.5 Messung der Zustellfrequenz

Um nicht nur beim Empfang, sondern bereits beim Versand Spam-E-Mails zu erkennen und zu blockieren, beschränken die meisten E-Mail-Dienstanbieter bei Privatkunden die Anzahl der versendeten Mails auf wenige Hundert pro Tag. Auf diese Weise sollen die durch Malware über „Zombie-PCs“ und ohne Wissen der Besitzer verschickten Spammails gestoppt werden.

Greylisting

Eine technische Maßnahme gegen unerwünschte E-Mails, die sich in der Praxis bislang als sehr erfolgreich erwiesen hat, ist das Greylisting. Dieses Verfahren nutzt die bei den Spam-Versendern vorherrschende mangelnde Fehlertoleranz.[86] Erfolgreiches Spammen setzt voraus, dass innerhalb sehr kurzer Zeit viele Millionen E-Mails versendet werden. Ein Großteil dieser Mails wird an Adressen verschickt, die per Zufallsprinzip generiert wurden und die nicht existieren. Aus diesem Grund erscheint es aus Sicht der Spam-Versender nicht sinnvoll, fehlgeschlagene Zustellversuche zu wiederholen, denn dies würde unverhältnismäßig hohe Rechnerkapazitäten erfordern.

Diese Tatsache machen sich Mailserver mit Greylisting zunutze. Bevor der Inhalt einer Mail akzeptiert wird, werden bei einem Verbindungsversuch zunächst die drei Informationen IP-Adresse des kontaktaufnehmenden Hosts, die Envelope-Adresse des Absenders sowie die Envelope-Adresse des Empfängers gespeichert und analysiert. Wird diese Dreierkombination zum ersten Mal registriert, so wird der Zustellversuch mit einer temporären Fehlermeldung „450 you are greylisted – try again later“ abgelehnt. Mailserver, die nicht dem Massenversand dienen, unternehmen in der Regel nach dieser Fehlermeldung weitere Zustellversuche.

Nach einer definierten Zeit von beispielsweise 10 Minuten wird das Eingangs-Gateway des E-Mail-Servers für Mails mit dieser Dreierkombination freigeschaltet, so dass eine Zustellung erfolgt. Erfolgt während der nächsten 12 Stunden ein Zustellungsversuch mit derselben Kombination, so werden alle E-Mails mit dieser Dreierkombination für 36 Tage frei geschaltet.

Auf diese Weise wird die E-Mail-Kommunikation mit regelmäßigen Kommunikationspartnern nicht gestört, während die unerwünschten Massensendungen abgehalten werden. Mailserver aus Domains, von denen keine Spam-E-Mails zu erwarten sind, können zudem von dieser Greylisting-Prozedur ausgeschlossen werden.

Probleme können dann auftreten, wenn dynamische IP-Adressen verwendet werden, beispielsweise bei der Modemeinwahl. Hier ist ein Absender unter Umständen nicht lange genug mit der gleichen IP-Adresse im Netz, um die Kriterien für eine erfolgreiche

---

86 Vgl. Völker (2004), S. 94ff.

Zustellung zu erfüllen. Abhilfe schafft in diesen Fällen das Versenden der Mail über das Relay eines E-Mail-Providers, das wiederum über eine permanente IP-Adresse verfügt.

Im praktischen Einsatz lässt sich mit dem Greylisting das Aufkommen von unerwünschten Massen-E-Mails deutlich reduzieren, ohne dass erwünschte E-Mails verloren gehen. An der Universität Würzburg konnte der Anteil an Spam-Mails am gesamten Mailaufkommen beispielsweise von über 90% auf rund 35% reduziert werden. Dies führt nicht nur zu gewichtigen Einsparungen von Speicherkapazität sondern reduziert auch die gefährlichen E-Mail-Würmer, die auf die gleiche Weise wie Spam-Mails versendet werden.

Allerdings trägt Greylisting nicht dazu bei, den Datenverkehr durch unerwünschte Nachrichten zu reduzieren. Im Gegenteil, durch die erforderlichen mehreren Zustellversuche wird der Verkehr sogar erhöht.

7.4.6 Herausforderungen der technischen Spam-Bekämpfung

Idealerweise sollten unerwünschte Massenaussendungen direkt an ihrer Quelle gestoppt werden. Ein Ansatz hierzu wäre es, die wirtschaftlichen Anreize für das Spamming zu unterbinden, beispielsweise durch kostenpflichtige „Mail-Briefmarken“. Dabei liefe man aber Gefahr, die Vorteile der freien und kostengünstigen Kommunikation über dezentral organisierte elektronische Netze zu vermindern. Auch kartellrechtliche Bedenken stehen einem derartigen Vorgehen entgegen.

Ein weiterer Ansatz, unerwünschte Massenaussendungen direkt an der Quelle zu stoppen, ist die Aufhebung der Anonymität der Absender. Dies ist jedoch mit dem derzeitigen E-Mail-Protokoll (SMTP) nicht möglich, da zahlreiche Möglichkeiten der Identitätsverschleierung existieren. Ein neues Mailprotokoll mit Authentisierungsmechanismen erscheint allenfalls mittel- bis langfristig durchsetzbar.

Als Second Best Ansatz erweist sich gegenwärtig daher eine simultane Bekämpfung von unerwünschten Massenaussendungen an mehreren Fronten: Gesetzliche Regelungen, deren konsequente Anwendung, Selbstregulierungsvereinbarungen der Industrie, technische Maßnahmen zur Filterung und schließlich Information der Nutzer über bewusstes Verhalten.

7.5 Nutzerverhalten

Damit Anti-Spam-Maßnahmen greifen können, ist es unabdingbar, die Nutzer in den Maßnahmenkatalog einzubeziehen. Dies gilt sowohl auf gesamtgesellschaftlicher Ebene als auch konkret in Betrieben und Verwaltungen.

Zunächst erscheint es bedeutsam, die privaten und geschäftlichen E-Mail-Nutzer über die Risiken des Spam zu informieren. Dazu gehört vor allem Aufklärung über diejenigen Betrugsversuche, die für einzelne Nutzer hohe Kosten verursachen können. Wichtig ist demnach, über gängige Praktiken wie Rufnummernmissbrauch, illegalen Medikamentenverkauf, Vorkasse-Betrug etc. zu informieren. Es sollte dabei nicht außer Acht gelassen werden, dass trotz hoher Online-Verbreitung in den Haushalten, Unternehmen oder Schulen dennoch eine relevante Anzahl von unerfahrenen bzw. neuen E-Mail-Kunden das Internet nutzt und diese Gruppe für Spam-Betrügereien besonders empfänglich sein dürfte. Eine regelmäßige und nachhaltige Informationspolitik von verschiedenen Akteuren wie etwa Bundesnetzagentur, ISP, Verbraucherschutzorganisationen oder auch Aus- und Weiterbildungsinstitutionen ist daher wünschenswert.[87]

Des weiteren sollten die Nutzer auf individuelle Verhaltensmaßnahmen aufmerksam gemacht werden, die die Wirksamkeit der übergeordneten Anti-Spam-Maßnahmen erhöht. Dazu gehört u.a.:

- nicht auf Spam-Mails zu antworten und auch keine scheinbaren Opt-out Links anzuklicken. Dies bestätigt dem Spammer die Existenz des Accounts.
- rechtlich gegen den Versender vorzugehen (Unterlassungsansprüche nach § 823 Abs. 2 i. V. m. § 1004 BGB geltend machen). Dies ist allerdings schwierig, da die Identität des Spammers festgestellt werden muss.
- die Beschwerdestellen der Bundesnetzagentur oder des Aktionsbündnisses gegen Spam zu nutzen. Die Weiterleitung von Spam an die Beschwerdestelle ermöglicht den Verbänden, einen Unterlassungsanspruch nach UWG (§ 8 Abs. 1 UWG) geltend zu machen (§ 8 Abs. 3 Nr. 2-4 UWG).
- die eigene E-Mail-Adresse nicht wahllos weiterzugeben oder auf einer Website zu veröffentlichen. Schon die Verfremdung der Adresse als me at provider.de (statt me@provider.de) schützt vor automatisiertem „harvesting“ der Adresssammler.[88]
- für das Abonnement von Newslettern u.ä. „Wegwerf-Adressen“ zu registrieren, die beispielsweise über den Dienst www.spamgourmet.com erhältlich sind. Sie werden nur bis zu zwanzig Mal verwendet und verlieren dann ihre Gültigkeit.
- E-Mail-Programme mit Filterfunktionen zu verwenden.

---

87 Im Netz finden sich beispielsweise auf den Homepages der Bundesnetzagentur, der Wettbewerbszentrale und auch von VZBV und Eco sowie BMWi Hinweise zum Umgang mit Spam.

88 Laut einer Untersuchung des US-amerikanischen FTC werden solche Adressen so gut wie niemals als Spam-Adresse entdeckt (FTC Press Release, November 28, 2005, „FTC Study Shows Technology Gaining in the Battle Against Spam”).

8 Fazit

Unerwünschte Massenaussendungen besitzen per Definition kommerziellen Charakter und werden über die verschiedensten Medien versandt (Telefon, Fax, Post, E-Mail). Besonders belästigend wird von den Nutzern unerwünschte E-Mail bewertet. Spam macht heute bis zu 80 Prozent aller versandten E-Mails aus. Dies bedeutet ein Spam-Aufkommen von schätzungsweise 48 Mrd. weltweit pro Tag in 2005.

Seriöses Direktmarketing über E-Mail stellt demgegenüber einen wichtigen Zweig der Werbewirtschaft dar. Im Jahr 2003 wurden 1,9 Mrd. Euro in diese Werbeform investiert und über 11 Mrd. Euro in weitere Internet-Werbung, Banner und Werbung mit Response-Elementen. Auch in Zukunft ist mit einer Fortsetzung dieses Trends und somit einem hohen Interesse der Werbetreibenden zu rechnen, diese kostengünstige Werbeform, über die spezifische Zielgruppen besonders effektiv erreicht werden können, zu erhalten.

Spam wird zwar auch mit legalem Inhalt (Werbebotschaften) versandt, der Großteil besteht jedoch aus Botschaften mit illegalem Inhalt und kann mittels Inhaltsanalyse relativ einfach identifiziert werden. Pornographie und Werbung für Medikamente sowie Finanzdienstleistungen machen einen erheblichen Teil des Spam aus: Insgesamt rd. 57 Prozent der unerwünschten E-Mails entfallen hierauf. Der Anteil von Werbung für Medikamentenverkauf beläuft sich auf rund ein Fünftel des gesamten Spam-Aufkommens. Hinzu kommen rund 10 Prozent allein für Viagra-Werbung. Ein weiterer großer Anteil von Spam entfällt auf Werbung für (illegale) Softwarekopien (rd. 7 Prozent).

Der Großteil des Spam stammt aus den USA sowie Südkorea. Nur etwa 2 Prozent werden von Deutschland aus verschickt. Diese Tatsache erschwert die strafrechtliche Verfolgung der Spammer erheblich. Phishing Websites werden ebenfalls hauptsächlich in den USA gehostet (37%) und in China/Taiwan/Hongkong (28%). Auch in diesem Bereich stammen nur etwa 3 Prozent der Phishing Websites von Betrügern innerhalb Deutschlands. Eine strafrechtliche Verfolgung von Spammern ist somit nur in internationalen Kooperationen sinnvoll.

Eine für die Nutzer häufig mit hohen Schäden verbundene Art von Spam ist das Rufnummern-Spamming. In Einzelfällen summiert sich der Schaden auf mehrere Tausend Euro pro Telefonrechnung, wenn der Geschädigte eine der MWD-Nummern zurückruft. Die Anzahl der Beschwerden bei der zuständigen Behörde nimmt seit Jahren kontinuierlich zu. Da Nummern national vergeben werden und daher die Verursacher in der Regel identifizierbar sind, ist die Verfolgung vergleichsweise leicht möglich. Auf Grundlage des TKG und des MWD-Gesetzes ist die BNetzA befugt, gegen den Missbrauch von Rufnummern, insbesondere von 0190er/090er Mehrwertdiensterufnummern, vorzugehen. Die möglichen Sanktionen werden zahlreich eingesetzt. Teilweise reichen sie jedoch nicht aus, um eine abschreckende Wirkung für Spammer zu entfalten. Häufig

werden z. B. nach Abschaltung von Nummern sofort neue beantragt und das Spamming fortgesetzt. Drastischere Strafen könnten hier Abhilfe schaffen.

Aufgrund der geringen Kosten für den Versand von E-Mails existieren hohe Anreize, das Medium für den Versand unerwünschter Werbemails zu missbrauchen. Bei einem seriösen, hochwertigen Massenversand per Post mit einer Auftragsspanne von 50 Euro müssen wenigstens 20 von 1.000 Adressaten das Angebot nachfragen, damit der Break-Even-Point der Werbeaussendung erreicht wird. Demgegenüber reichen bei E-Mail-Spam bereits 0,02 Kunden pro 1.000 Adressen und gleicher Auftragsspanne, um diese Grenze zu erreichen.

Es erscheint vor diesem Hintergrund wenig wahrscheinlich, dass das Spam-Aufkommen in absehbarer Zeit abnimmt. Vielmehr ist damit zu rechnen, dass Effizienzgewinne durch E-Mail wie etwa geringe Kosten, rasche Übertragung, Entfernungsunabhängigkeit und Beschleunigung von Koordinations- und Organisationsprozessen durch systemimmanente Nachteile wie geringe Verlässlichkeit, unzureichende Integrität der Daten, mangelnde Vertraulichkeit und Missbrauch konterkariert werden.

Hohe Kosten für die Nutzung des offenen, dezentralen E-Mail-Systems, z.B. Überwachungs- und Durchsetzungskosten (verursacht durch Spam) können zu Ausweichreaktionen führen, d.h. zur Nutzung zentral-hierarchisch organisierter Kommunikationsmittel mit geringeren Kosten für den Nutzer. Der Grund dafür ist darin zu suchen, dass Unternehmen nach der Transaktionskostentheorie nur so viele Transaktionen übernehmen, bis ihre Kosten für eine weitere Transaktion den Kosten der Abwicklung über den Markt bzw. den Kosten einer anderen Unternehmung entsprechen (Prinzip der marginalen Substitution). Die Erhöhung der Transaktionskosten durch Spamming liegt vor allem in den folgenden Punkten begründet:

- Übertragungskosten,
- Arbeitszeit für manuelle Selektion,
- Risiko, erwünschte E-Mails irrtümlich als Spam auszusortieren (False Positives) bzw. Übersehen von E-Mails in der Spam-Flut,
- Risiko von Malware (Würmer, Trojaner, Viren),
- Risiko unseriöser Angebote, insbesondere bei Rufnummern-Spam,
- Kosten für Anti-Spam-Maßnahmen und Authentifizierungsmaßnahmen,
- genereller Verlust an Verlässlichkeit von E-Mail und fallweise Substitution durch andere Medien (Fax, Briefpost).

Schätzungen gehen von einem Anteil von 70 bis 80 Prozent Spam bei E-Mails aus. Für Deutschland bedeutet dies, dass ca. 500 Mio. Spam-Mails pro Woche an deutsche U-

ser versandt werden und dadurch Transaktionskosten bei ISP, Unternehmen und Verbrauchern entstehen.

Die höchsten Einzelschäden, insbesondere für private Nutzer, entstehen durch Rufnummernmissbrauch und Phishing. Rufnummern-Spamming verursacht nach Schätzungen des BKA ca. 30 bis 250 Euro Schaden pro Fall. In Einzelfällen sind Personen um 0,75 Mio. Euro durch Dialer geschädigt worden. Schäden durch Phishing werden in Deutschland auf etwa 4,5 Mio. Euro pro Jahr beziffert.

Neben den direkten Kosten, die durch Schäden unmittelbar entstehen, ist Spam die Ursache für indirekte Kosten, die sich für den einzelnen privaten oder geschäftlichen Nutzer oder auch für ISP auswirken. Diese Kosten addieren sich auf volkswirtschaftlicher Ebene zu Summen im Milliardenbereich, wie Studien in den USA sowie der EU zeigen.

Für die Nutzer entstehen z. B. Kosten für die Einrichtung und Pflege von Spam-Filtern für Mail-Clients, SW und HW Spam-Filtern für Mailserver, das Sortieren von False Positives mit dem entsprechenden Arbeitzeitaufwand sowie für das Anwenden verbraucherschutzrechtlicher Maßnahmen gegen Spam-Versender.

ISP werden durch den zusätzlich erforderlichen Traffic und Speicherplatz belastet. Auch für sie bedeutet die Entwicklung, Einrichtung, Pflege von Spam-Filtern (SW, HW) zusätzlichen Aufwand. Kosten entstehen außerdem durch die erforderliche rechtliche Beratung über den Einsatz von Anti-Spam-Maßnahmen sowie Maßnahmen gegen Spam-Versender, Presse- und Marketingaktionen, um über Anti-Spam-Maßnahmen zu informieren und durch die Organisation von anbieterübergreifenden Arbeitsgruppen und die Ausarbeitung von Anti-Spam-Strategien.

Die volkswirtschaftlichen Kosten für Spam und andere Formen von unerwünschten Massenaussendungen haben in den letzten Jahren in starkem Umfang zugenommen, so dass dringender Handlungsbedarf auf nationaler und internationaler Ebene besteht. Zahlreiche Akteure und neugegründete Initiativen haben sich des Problems angenommen. Durch Aktivitäten auf verschiedenen Ebenen – politisch, rechtlich, sozial – versuchen sie, die beeinträchtigte Funktionabilität und Verlässlichkeit von E-Mail zu vermindern, die durch Spam verursachten Kosten für ISP und Nutzer zu verringern und gleichzeitig das Internet als Form des Direktmarketings zu erhalten. Dabei ist allgemein die Einstellung vorherrschend, dass eine Verminderung des Spam nur durch ein Zusammenspiel von Gegenmaßnahmen auf allen Ebenen möglich ist. Dazu gehören internationale Kooperationen genauso wie Gesetze und regulatorische Maßnahmen auf nationaler Ebene, Selbstregulierung, technische Maßnahmen und intensive Nutzerinformation.

Auf nationaler Ebene wurden Gesetze und regulatorische Maßnahmen ergriffen, die die entsprechenden EU-Richtlinien umsetzen. Dazu gehört in Deutschland die Novellierung des UWG. Um Rufnummern-Spamming gezielt zu bekämpfen, wurde das Mehrwert-

dienste-Gesetz (MWD-Gesetz) verabschiedet. Ergänzt werden diese Maßnahmen durch selbstregulative Initiativen der Verbände wie etwa die Beschwerde-Hotlines von Eco, VZBV, WBZ, die Einführung von Whitelists (Certified Senders Alliance mit Code of Conduct) auf Initiative des Eco und des Direktmarketingverbands, das „Aktionsbündnis gegen Spam“, welches ein koordiniertes rechtliches Vorgehen zum Ziel hat und der Förderung des internationalen Austauschs und der Strategieplanung zwischen den Verbänden weltweit dient.

Die globale Dimension der Kommunikationsnetze und der Spam-Problematik erfordern internationale Abstimmungsprozesse in der Spamabwehr. Auf Ebene der Anti-Spam-Gesetzgebung besteht das Ziel, die weißen Flecken in der Gesetzgebung gegen Spam weltweit zu beseitigen. Auf Ebene der Gesetzesanwendung ist eine internationale Zusammenarbeit der zuständigen Behörden anzustreben. Auf internationaler Ebene sind insbesondere die Kooperations- und Informationsanstrengungen des UN World Summit of the Information Society (WSIS), der Informationsaustausch auf ITU-Ebene, das OECD Anti-Spam Toolkit, der London Action Plan sowie die EU Datenschutzrichtlinie 2002 und das Contact Network of Spam Enforcement Authorities – CNSA zu nennen. Neben der gegenseitigen Information über Best-Practice-Lösungen und dem Schaffen von Transparenz über die in den einzelnen Ländern jeweils zuständigen Institutionen dienen diese Aktivitäten vor allem dazu, eine Kooperation der Strafverfolgungsbehörden angesichts der zunehmenden Organisiertheit der Kriminalitätsform „Spam“ zu erleichtern.

Technische Maßnahmen bleiben die Grundlage für individuelle Bekämpfung von Spam. Die technische Unterscheidung von „Spam“ und „Ham“ beruht auf mehreren Merkmalen (bspw. IP-Adresse, Absenderadresse u. –domain, Inhalt, Menge und Frequenz). Besonders auf technischem Gebiet wird deutlich, dass keine Anti-Spam-Maßnahme für sich allein erfolgreich ist, sondern eine Kombination von technischen Maßnahmen sinnvoll ist. Technisches Filtering ist aber notwendigerweise durch händisches Sortieren zu ergänzen und so bleibt trotz immer weiter verbesserter Technologie der Zeit- und Kostenaufwand auch bei erhöhtem Technikeinsatz für jeden Nutzer erheblich.

Schließlich ist es wichtig, die privaten und geschäftlichen E-Mail-Nutzer über die Risiken des Spam zu informieren. Dazu gehört die Aufklärung über Betrugsversuche, über gängige Praktiken wie Rufnummernmissbrauch, illegalen Medikamentenverkauf, Vorkasse-Betrug etc. Eine regelmäßige und nachhaltige Informationspolitik von verschiedenen Akteuren wie etwa Bundesnetzagentur, ISP, Verbraucherschutzorganisationen oder auch Aus- und Weiterbildungsinstitutionen erscheint daher wünschenswert.

Um die Nutzer adäquat in das Netzwerk zur Spamabwehr einzubinden, ist es neben Aufklärungsmaßnahmen erforderlich, zentrale nationale Anlaufstellen – beispielsweise in Form einer E-Mail-Box – anzubieten, um die Beschwerden zu bündeln und den Aufwand bei der Ermittlung der Verursacher zu minimieren. Um eine hinreichende Nutzerakzeptanz dieser Beschwerdestellen zu erzielen, sollten nicht nur Beschwerden gegen

Verstöße nationaler Gesetze entgegengenommen und behandelt werden, sondern auch gegen unerwünschte Massenaussendungen aus dem Ausland, die das Gros dieser Aussendungen darstellen.

Abschließend bleibt zu konstatieren, dass Spam-Versender weltweit agieren, Massenaussendungen zu äußerst geringen Kosten realisieren, trotz geringer Rücklaufquote hohe wirtschaftliche Anreize besitzen, Spam zu versenden, ihre Identität mit einfachen Mitteln verschleiern können sowie innovativ und einfallsreich bei der Umgehung von Abwehrmaßnahmen und beim Einsatz neuester Technologie sind. Der Kampf gegen Spam wird vor diesem Hintergrund zu einer dauerhaften Aufgabe verschiedenster Akteure.

Interventionsstrategien sollten vor allem die Funktionabilität und Verlässlichkeit der Dienste gewährleisten, die Kosten für die Nutzung gering halten, die Belange der seriösen Werbewirtschaft und der Wachstumsbranchen E-Commerce und Mehrwertdienste schützen, an vielen Fronten effektiv und dauerhaft greifen (international/national, technisch-organisatorisch) und alle Akteure (private und geschäftliche Nutzer, ISP, Institutionen) einbeziehen.

Neben Gesetzen sind weitere Maßnahmen sinnvoll wie die Etablierung weiterer Sanktionsmaßnahmen mit abschreckender Wirkung, die kontinuierliche Schulung und Aufklärung der Nutzer, eine regelmäßige Weiterentwicklung der technischen Lösungen, ggf. durch öffentlich geförderte Institutionen, die Forcierung von Selbstregulierungsmaßnahmen (Verhaltenskodizes, Gütesiegeln, Acceptable Use Policies etc.) und eine regelmäßige Erfolgskontrolle in Bezug auf die bestehenden Maßnahmen. Durch Selbstregulierungsvereinbarungen der Industrie können zum einen, wie im Falle der Codes of Conduct der Direktvermarkter, die Mengen an unerwünschten Massensendungen reduziert werden. Zum anderen ermöglicht ein effizient organisierter internationaler Abgleich von Black- und Whitelists den ISP, ihre Spamfilter zeitnah zu optimieren.

Einige offene Aspekte werden in Zukunft diskutiert werden müssen, um Spam nachhaltig zu bekämpfen. Dazu gehört u. a. die Frage, ob nach der „Spam-Flut“ eine „Beschwerde-Flut“ einsetzen wird, und wie die neu gegründeten Organisationen mit dieser umgehen können. Des Weiteren wird künftig zu erörtern sein, ob die ersten Erfolge der Spam-Bekämpfung von Dauer sein werden, wenn sich die Spam-Versender weiter „professionalisieren“.

Literaturverzeichnis

Asscher, Lodewijk F. und J van Erve (2004): Regulating Spam. Directive 2002/58 and beyond, Institute for Information Law (IViR), University of Amsterdam

Barrett, D. J. (1996): Gauner und Ganoven im Internet, Bonn

BMWA (2005): EB-Kommunikation und Spam, in: e-facts, Ausgabe 17, November 2004

Bössmann, E. (1981): Weshalb gibt es Unternehmungen? Der Erklärungsansatz von Ronald H. Coase, in: Zeitschrift für die gesamte Staatswissenschaft, Vol. 137, S. 667 - 674

Brodersen, B. (2004), Wird Spam zur neuen Plage für VoIP-Telefonierer? Software-Firmen arbeiten an Anti-Spam-Filtern, www.teltarif.de/intern/action/print/arch/2004/kw39/s14971.html

BSI (2005): Antispam-Strategien. Unerwünschte E-Mails erkennen und abwehren, Bonn

Coase, R. H. (1937): The Nature of the Firm, in Economica, Vol. 4, S. 386 - 405

DDV (2004): Direkt zum Kunden. Erfolgsfaktoren, Checklisten und Partner für Direct Mail-Aktionen, Blickpunkt Dialog 2004

Dietrich, Chr. und N. Pohlmann (2004): E-Mail-Verlässlichkeit: Auswertung der Umfrage Ende 2004, ifis - Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen

DIHK - Deutscher Industrie- und Handelskammertag (2004): Spam-E-Mails - Wie die Flut eingedämmt werden kann, Berlin

Eco - Verband der deutschen Internetwirtschaft (2004): White Paper der Anti Spam Task Force – ASTF, Köln 21.09.2004

FTC (2003): False Claims in Spam, 29 April 2003

Godin, S. (2001): Permission Marketing, FinanzBuchVerlag 2001

Graydon, A. (2005), Protokollfragen. VoIP-Security bei SIP & Co., in: Kes, Die Zeitschrift für Informationssicherheit, Nr. 2, Mai 2005, S. 58-59

Gutsche, O. (2003): Die Umsetzung der E-Commerce-Richtlinie in der Bundesrepublik Deutschland und in der Republik Österreich, Magisterarbeit an der Universität Leipzig

Hölscher, U. (1991): Kalkulation einer Direktwerbe-Aktion, in: Dallmer, Heinz (Hrsg.) Handbuch Direct Marketing, Wiesbaden, S. 535-543

Honeynet Project and Research Alliance (2005a): Know your Enemy: Tracking Botnets. Using honeynets to learn more about Bots, Stand: 13. März 2005, http://www.honeynet.org

Honeynet Project and Research Alliance (2005b): Setup of the honeynet. Stand: Juni 2005, http://www-i4.informatik.rwth-aachen.de/lufg/research/projects/honeynet/honey-setup.en.html

ICANN (2005): Community Experiences with the InterNIC Whois Data Problem Reports System, 31 March 2005

IETF, Positionspapier Jonathan Rosenberg und Cullen Jennings

John R. L., M. Levine-Young, R. Everett-Church: Spam bekämpfen für Dummies, mitp 2002

Kaestner, J. und N. Tews (2004): Werbung und Wettbewerbsrecht. Einführung in die Grundlagen des Lauterkeitsrechts, 2., völlig neu bearbeitete Auflage, Bad Homburg v. d. Höhe

Keber, T. (2004): Neues zu Spam: Ein lang ersehntes Urteil des Bundesgerichtshofes, die Richtlinie 2002/58/EG und die UWG-Novelle, JurPC 6/2004, online abrufbar unter: www.jurpc.de/aufsatz/20040218.htm

Kellner A. (2002): Short guide: permission-e-mailmarketing. Mit Erlaubnis zum Erfolg. BoD GmbH, Norderstedt 2002

Köcher, J. K. (2005): Strafbarkeit der Ausfilterung von E-Mails, Anmerkungen zum Beschluss des OLG Karlsruhe vom 10.01.2005 – 1 Ws 152/04, in: DuD 29 (2005), Heft 3, S. 163 – 165

Kommission der Europäischen Gemeinschaften (2004): Mitteilung der Kommission an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über unerbetene Werbenachrichten (Spam), KOM(2004) 28 endgültig, Brüssel, 22.01.2004

Kroll, R. (1991): Direct Marketing für Lotterien, in: Dallmer, Heinz (Hrsg.) Handbuch Direct Marketing, Wiesbaden, S. 759-768

Lutz, F. (2005), Lauschangriff. Wanze over IP, in: kes, Die Zeitschrift für Informationssicherheit, Nr. 2, Mai 2005, S. 55-57

OECD (2005): Anti-Spam Regulation, DSTI/CP/ICCP/SPAM(2005)10/FINAL, 15.11.2005

PEW Internet & American Life Project (2005): CAN-SPAM a year later, http://www.pewinternet.org/pdfs/PIP_Spam_Ap05.pdf

Radermacher, A. T. (2004): Spam Prevention in Voice over IP Networks, Diplomarbeit, Salzburg

RegTP (2005): Jahresbericht 2004 der Regulierungsbehörde für Telekommunikation und Post gemäß § 122 Telekommunikationsgesetz, Bonn

RegTP (2005): Maßnahmenliste Spam, www.regtp.de

Richter, R. und E. Furubotn (1996): Neue Institutionenökonomik, Tübingen

Schwarz, T. (2004) : Leitfaden eMail Marketing und Newsletter-Gestaltung. Waghäusl 2004

Vick, J. und F. Roters (2003): Account-Missbrauch im Internet, Bundeskriminalamt Kriminalistisches Institut (Hg.), Wiesbaden

Völker, R. (2004): Moment bitte. Mit Greylisting gegen Spam vorgehen, in: iX 12/2004, S. 94-98

Wehr, H. (2003): Nie wieder Spam! Kampf den Werbemails. Markt+Technik 2003.

ZAW (2005): ZAW-Jahrbuch "Werbung in Deutschland 2005", Berlin

Als "Diskussionsbeiträge" des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste sind zuletzt erschienen:

Nr. 190: Rudolf Pospischil:

Repositionierung von AT&T - Eine Analyse zur Entwicklung von 1983 bis 1998, Dezember 1998

Nr. 191: Alfons Keuter:

Beschäftigungseffekte neuer TK-Infrastrukturen und -Dienste, Januar 1999

Nr. 192: Wolfgang Elsenbast:

Produktivitätserfassung in der Price-Cap-Regulierung – Perspektiven für die Preisregulierung der Deutschen Post AG, März 1999

Nr. 193: Werner Neu, Ulrich Stumpf, Alfons Keuter, Lorenz Nett, Cara Schwarz-Schilling:

Ergebnisse und Perspektiven der Telekommunikationsliberalisierung in ausgewählten Ländern, April 1999

Nr. 194: Ludwig Gramlich:

Gesetzliche Exklusivlizenz, Universaldienstpflichten und "höherwertige" Dienstleistungen im PostG 1997, September 1999

Nr. 195: Hasan Alkas:

Rabattstrategien marktbeherrschender Unternehmen im Telekommunikationsbereich, Oktober 1999

Nr. 196: Martin Distelkamp:

Möglichkeiten des Wettbewerbs im Orts- und Anschlußbereich des Telekommunikationsnetzes, Oktober 1999

Nr. 197: Ulrich Stumpf, Cara Schwarz-Schilling unter Mitarbeit von Wolfgang Kiesewetter:

Wettbewerb auf Telekommunikationsmärkten, November 1999

Nr. 198: Peter Stamm, Franz Büllingen:

Das Internet als Treiber konvergenter Entwicklungen – Relevanz und Perspektiven für die strategische Positionierung der TIME-Player, Dezember 1999

Nr. 199: Cara Schwarz-Schilling, Ulrich Stumpf:

Netzbetreiberportabilität im Mobilfunkmarkt – Auswirkungen auf Wettbewerb und Verbraucherinteressen, Dezember 1999

Nr. 200: Monika Plum, Cara Schwarz-Schilling:

Marktabgrenzung im Telekommunikations- und Postsektor, Februar 2000

Nr. 201: Peter Stamm:

Entwicklungsstand und Perspektiven von Powerline Communication, Februar 2000

Nr. 202: Martin Distelkamp, Dieter Elixmann, Christian Lutz, Bernd Meyer, Ulrike Schimmel:

Beschäftigungswirkungen der Liberalisierung im Telekommunikationssektor in der Bundesrepublik Deutschland, März 2000

Nr. 203: Martin Distelkamp:

Wettbewerbspotenziale der deutschen Kabel-TV-Infrastruktur, Mai 2000

Nr. 204: Wolfgang Elsenbast, Hilke Smit:

Gesamtwirtschaftliche Auswirkungen der Marktöffnung auf dem deutschen Postmarkt, Mai 2000

Nr. 205: Hilke Smit:

Die Anwendung der GATS-Prinzipien auf dem Postsektor und Auswirkungen auf die nationale Regulierung, Juni 2000

Nr. 206: Gabriele Kulenkampff:

Der Markt für Internet Telefonie - Rahmenbedingungen, Unternehmensstrategien und Marktentwicklung, Juni 2000

Nr. 207: Ulrike Schimmel:

Ergebnisse und Perspektiven der Telekommunikationsliberalisierung in Australien, August 2000

Nr. 208: Franz Büllingen, Martin Wörter:

Entwicklungsperspektiven, Unternehmensstrategien und Anwendungsfelder im Mobile Commerce, November 2000

Nr. 209: Wolfgang Kiesewetter:

Wettbewerb auf dem britischen Mobilfunkmarkt, November 2000

Nr. 210: Hasan Alkas:

Entwicklungen und regulierungspolitische Auswirkungen der Fix-Mobil Integration, Dezember 2000

Nr. 211: Annette Hillebrand:

Zwischen Rundfunk und Telekommunikation: Entwicklungsperspektiven und regulatorische Implikationen von Webcasting, Dezember 2000

Nr. 212: Hilke Smit:

Regulierung und Wettbewerbsentwicklung auf dem neuseeländischen Postmarkt, Dezember 2000

Nr. 213: Lorenz Nett:

Das Problem unvollständiger Information für eine effiziente Regulierung, Januar 2001

Nr. 214: Sonia Strube:

Der digitale Rundfunk - Stand der Einführung und regulatorische Problemfelder bei der Rundfunkübertragung, Januar 2001

Nr. 215: Astrid Höckels:

Alternative Formen des entbündelten Zugangs zur Teilnehmeranschlussleitung, Januar 2001

Nr. 216: Dieter Elixmann, Gabriele Kulenkampff, Ulrike Schimmel, Rolf Schwab:

Internationaler Vergleich der TK-Märkte in ausgewählten Ländern - ein Liberalisierungs-, Wettbewerbs- und Wachstumsindex, Februar 2001

Nr. 217: Ingo Vogelsang:

Die räumliche Preisdifferenzierung im Sprachtelefondienst - wettbewerbs- und regulierungspolitische Implikationen, Februar 2001

Nr. 218: Annette Hillebrand, Franz Büllingen:

Internet-Governance - Politiken und Folgen der institutionellen Neuordnung der Domainverwaltung durch ICANN, April 2001

Nr. 219: Hasan Alkas:

Preisbündelung auf Telekommunikationsmärkten aus regulierungsökonomischer Sicht, April 2001

Nr. 220: Dieter Elixmann, Martin Wörter:

Strategien der Internationalisierung im Telekommunikationsmarkt, Mai 2001

Nr. 221: Dieter Elixmann, Anette Metzler:

Marktstruktur und Wettbewerb auf dem Markt für Internet-Zugangsdienste, Juni 2001

Nr. 222: Franz Büllingen, Peter Stamm:

Mobiles Internet - Konvergenz von Mobilfunk und Multimedia, Juni 2001

Nr. 223: Lorenz Nett:

Marktorientierte Allokationsverfahren bei Nummern, Juli 2001

Nr. 224: Dieter Elixmann:

Der Markt für Übertragungskapazität in Nordamerika und Europa, Juli 2001

Nr. 225: Antonia Niederprüm:

Quersubventionierung und Wettbewerb im Postmarkt, Juli 2001

Nr. 226: Ingo Vogelsang
unter Mitarbeit von Ralph-Georg Wöhrl

Ermittlung der Zusammenschaltungsentgelte auf Basis der in Anspruch genommenen Netzkapazität, August 2001

Nr. 227: Dieter Elixmann, Ulrike Schimmel, Rolf Schwab:

Liberalisierung, Wettbewerb und Wachstum auf europäischen TK-Märkten, Oktober 2001

Nr. 228: Astrid Höckels:

Internationaler Vergleich der Wettbewerbsentwicklung im Local Loop, Dezember 2001

Nr. 229: Anette Metzler:

Preispolitik und Möglichkeiten der Umsatzgenerierung von Internet Service Providern, Dezember 2001

Nr. 230: Karl-Heinz Neumann:

Volkswirtschaftliche Bedeutung von Resale, Januar 2002

Nr. 231: Ingo Vogelsang:

Theorie und Praxis des Resale-Prinzips in der amerikanischen Telekommunikationsregulierung, Januar 2002

Nr. 232: Ulrich Stumpf:

Prospects for Improving Competition in Mobile Roaming, März 2002

Nr. 233: Wolfgang Kiesewetter:

Mobile Virtual Network Operators – Ökonomische Perspektiven und regulatorische Probleme, März 2002

Nr. 234: Hasan Alkas:

Die Neue Investitionstheorie der Realoptionen und ihre Auswirkungen auf die Regulierung im Telekommunikationssektor, März 2002

Nr. 235: Karl-Heinz Neumann:

Resale im deutschen Festnetz, Mai 2002

Nr. 236: Wolfgang Kiesewetter, Lorenz Nett und Ulrich Stumpf:

Regulierung und Wettbewerb auf europäischen Mobilfunkmärkten, Juni 2002

Nr. 237: Hilke Smit:

Auswirkungen des e-Commerce auf den Postmarkt, Juni 2002

Nr. 238: Hilke Smit:

Reform des UPU-Endvergütungssystems in sich wandelnden Postmärkten, Juni 2002

Nr. 239: Peter Stamm, Franz Büllingen:

Kabelfernsehen im Wettbewerb der Plattformen für Rundfunkübertragung - Eine Abschätzung der Substitutionspotenziale, November 2002

Nr. 240: Dieter Elixmann, Cornelia Stappen unter Mitarbeit von Anette Metzler:

Regulierungs- und wettbewerbspolitische Aspekte von Billing- und Abrechnungsprozessen im Festnetz, Januar 2003

Nr. 241: Lorenz Nett, Ulrich Stumpf unter Mitarbeit von Ulrich Ellinghaus, Joachim Scherer, Sonia Strube Martins, Ingo Vogelsang:

Eckpunkte zur Ausgestaltung eines möglichen Handels mit Frequenzen, Februar 2003

Nr. 242: Christin-Isabel Gries:

Die Entwicklung der Nachfrage nach breitbandigem Internet-Zugang, April 2003

Nr. 243: Wolfgang Briglauer:

Generisches Referenzmodell für die Analyse relevanter Kommunikationsmärkte – Wettbewerbsökonomische Grundfragen, Mai 2003

Nr. 244: Peter Stamm, Martin Wörter:

Mobile Portale – Merkmale, Marktstruktur und Unternehmensstrategien, Juli 2003

Nr. 245: Franz Büllingen, Annette Hillebrand:

Sicherstellung der Überwachbarkeit der Telekommunikation: Ein Vergleich der Regelungen in den G7-Staaten, Juli 2003

Nr. 246: Franz Büllingen, Annette Hillebrand:

Gesundheitliche und ökologische Aspekte mobiler Telekommunikation – Wissenschaftlicher Diskurs, Regulierung und öffentliche Debatte, Juli 2003

Nr. 247: Anette Metzler, Cornelia Stappen unter Mitarbeit von Dieter Elixmann:

Aktuelle Marktstruktur der Anbieter von TK-Diensten im Festnetz sowie Faktoren für den Erfolg von Geschäftsmodellen, September 2003

Nr. 248: Dieter Elixmann, Ulrike Schimmel with contributions of Anette Metzler:

"Next Generation Networks" and Challenges for Future Regulatory Policy, November 2003

Nr. 249: Martin O. Wengler, Ralf G. Schäfer:

Substitutionsbeziehungen zwischen Festnetz und Mobilfunk: Empirische Evidenz für Deutschland und ein Survey internationaler Studien, Dezember 2003

Nr. 250: Ralf G. Schäfer:

Das Verhalten der Nachfrager im deutschen Telekommunikationsmarkt unter wettbewerblichen Aspekten, Dezember 2003

Nr. 251: Dieter Elixmann, Anette Metzler, Ralf G. Schäfer:

Kapitalmarktinduzierte Veränderungen von Unternehmensstrategien und Marktstrukturen im TK-Markt, März 2004

Nr. 252: Franz Büllingen, Christin-Isabel Gries, Peter Stamm:

Der Markt für Public Wireless LAN in Deutschland, Mai 2004

Nr. 253: Dieter Elixmann, Annette Hillebrand, Ralf G. Schäfer, Martin O. Wengler:

Zusammenwachsen von Telefonie und Internet – Marktentwicklungen und Herausforderungen der Implementierung von ENUM, Juni 2004

Nr. 254: Andreas Hense, Daniel Schäffner:

Regulatorische Aufgaben im Energiebereich – ein europäischer Vergleich, Juni 2004

Nr. 255: Andreas Hense:

Qualitätsregulierung und wettbewerbspolitische Implikationen auf Postmärkten, September 2004

Nr. 256: Peter Stamm:

Hybridnetze im Mobilfunk – technische Konzepte, Pilotprojekte und regulatorische Fragestellungen, Oktober 2004

Nr. 257: Christin-Isabel Gries:

Entwicklung der DSL-Märkte im internationalen Vergleich, Oktober 2004

Nr. 258: Franz Büllingen, Annette Hillebrand, Diana Rätz:

Alternative Streitbeilegung in der aktuellen EMVU-Debatte, November 2004

Nr. 259: Daniel Schäffner:

Regulierungsökonomische Aspekte des informatorischen Unbundling im Energiebereich, Dezember 2004

Nr. 260: Sonja Schölermann:

Das Produktangebot von Universaldienstleistern und deren Vergleichbarkeit, Dezember 2004

Nr. 261: Franz Büllingen, Aurélia Gillet, Christin-Isabel Gries, Annette Hillebrand, Peter Stamm:

Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich, Februar 2005

Nr. 262: Oliver Franz, Marcus Stronzik:

Benchmarking-Ansätze zum Vergleich der Effizienz von Energieunternehmen, Februar 2005

Nr. 263: Andreas Hense:

Gasmarktregulierung in Europa: Ansätze, Erfahrungen und mögliche Implikationen für das deutsche Regulierungsmodell, März 2005

Nr. 264: Franz Büllingen, Diana Rätz:

VoIP – Marktentwicklungen und regulatorische Herausforderungen, Mai 2005

Nr. 265: Ralf G. Schäfer, Andrej Schöbel:

Stand der Backbone-Infrastruktur in Deutschland – Eine Markt- und Wettbewerbsanalyse, Juli 2005

Nr. 266: Annette Hillebrand, Alexander Kohlstedt, Sonia Strube Martins:

Selbstregulierung bei Standardisierungsprozessen am Beispiel von Mobile Number Portability, Juli 2005

Nr. 267: Oliver Franz, Daniel Schäffner, Bastian Trage:

Grundformen der Entgeltregulierung: Vor- und Nachteile von Price-Cap, Revenue-Cap und hybriden Ansätzen, August 2005

Nr. 268: Andreas Hense, Marcus Stronzik:

Produktivitätsentwicklung der deutschen Strom- und Gasnetzbetreiber – Untersuchungsmethodik und empirische Ergebnisse, September 2005

Nr. 269: Ingo Vogelsang:

Resale und konsistente Entgeltregulierung, Oktober 2005

Nr. 270: Nicole Angenendt, Daniel Schäffner:

Regulierungsökonomische Aspekte des Unbundling bei Versorgungsunternehmen unter besonderer Berücksichtigung von Pacht- und Dienstleistungsmodellen, November 2005

Nr. 271: Sonja Schölermann:

Vertikale Integration bei Postnetzbetreibern – Geschäftsstrategien und Wettbewerbsrisiken, Dezember 2005

Nr. 272: Franz Büllingen, Annette Hillebrand, Peter Stamm:

Transaktionskosten der Nutzung des Internet durch Missbrauch (Spamming) und Regulierungsmöglichkeiten, Januar 2006